虚拟专用网络

常见问题

文档版本	01
发布日期	2025-11-18

华为技术有限公司

版权所有 © 华为技术有限公司 2025。 保留一切权利。

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

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

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

 版权所有 © 华为技术有限公司

1 站点入云 VPN 企业版

1.1 热点问题

1.1.1 哪些设备可以与华为云进行 VPN 对接?

VPN支持标准IPsec协议，用户可以通过以下两个方面确认用户侧数据中心的设备能否与云进行对接：

1. 设备是否具备IPsec功能和授权：请查询设备的特性列表获取是否支持IPsec VPN。
2. 关于组网结构，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）也可以。

设备型号多为路由器、防火墙等，对接配置请参见**管理员指南**。

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。
- 与VPN服务做过对接测试厂商包括：
  - 设备厂商：华为（防火墙/AR）、山石（防火墙），CheckPoint（防火墙）。
  - 云服务厂商包括：阿里云，腾讯云，亚马逊（aws），微软（Microsoft Azure）。
  - 软件厂商包括：strongSwan。
- IPsec协议属于IETF标准协议，宣称支持该协议的厂商均可与云进行对接，用户不需要关注具体的设备型号。

  目前绝大多数企业级路由器和防火墙都支持该协议。
- 部分硬件厂商在特性规格列表中是宣称支持IPsec VPN的，但是需要专门购买软件License才能激活相关功能。

  请用户侧数据中心管理员根据设备具体型号与厂商进行确认。

 版权所有 © 华为技术有限公司

1.1.2 VPN 协商参数有哪些？默认值是什么？

表 1-1 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
	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。

版权所有 © 华为技术有限公司

协议	配置项	值
	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
	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。

版权所有 © 华为技术有限公司

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。
- 云侧不支持配置基于流量的IPsec SA生命周期，不会基于流量老化IPsec SA。

1.1.3 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。

1.1.4 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）。

1.1.5 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。

请用户在购买包年/包月VPN网关时，根据规划连通的数据中心数量选择合适的VPN连接数。

 版权所有 © 华为技术有限公司

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。

1.1.6 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。

VPN连接状态请在VPN连接“监控”列中单击 进行查看。

1.1.7 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。

1.1.8 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。

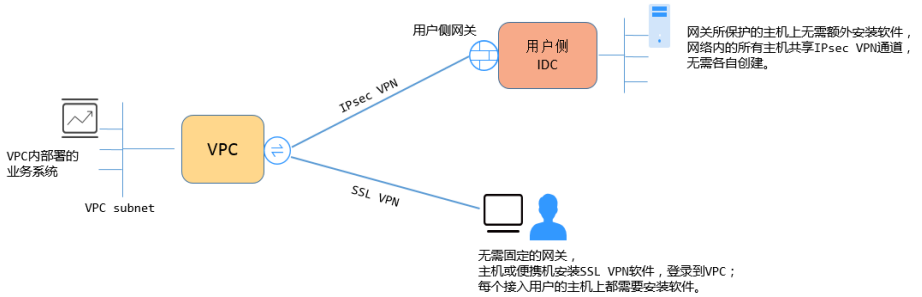
SSL VPN：连通的是一个客户端到一个局域网络，如出差员工的便携机访问公司内网。

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。

 版权所有 © 华为技术有限公司



说明

VPN支持IPsec VPN和SSL VPN。

1.1.9 IPsec VPN 是否会自动建立连接?

支持自动建立连接。

1.1.10 创建 VPN 都会产生哪些费用，VPN 网关 IP 收费吗?

VPN计费模式分为包年/包月和按需两种，费用包含：

- VPN网关费用
- VPN连接费用

  默认提供10条免费的VPN连接；超过10条后需要付费购买。
- VPN网关弹性公网IP带宽费用

  网关带宽的计费又可分为按流量或按带宽计费。

  a. 包年/包月计费模式下不可选择按流量计费。如果您选择包年/包月模式创建VPN，在创建网关阶段一次性收取网关带宽费用和连接的费用，用户后续创建VPN连接时不再收取费用。

  b. 按需方式为先使用后付费模式，计费周期为1小时。如果您选择按需模式创建VPN，页面会提示同时创建连接，费用包含了网关带宽费用和10个连接组费用，您在创建第11个连接时组时只产生连接的费用。

  说明

  VPN网关的带宽费用是独立的，与ECS绑定的EIP带宽相互独立，无法共享。

1.1.11 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。

1.1.12 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。

查询VPN网关监控状态，请在VPN网关“网关IP”列中单击EIP后面的 进行查看。

VPN连接

 版权所有 © 华为技术有限公司

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。

查询VPN连接监控状态，请在VPN连接“监控”列中单击 进行查看。

1.1.13 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。

1.1.14 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。

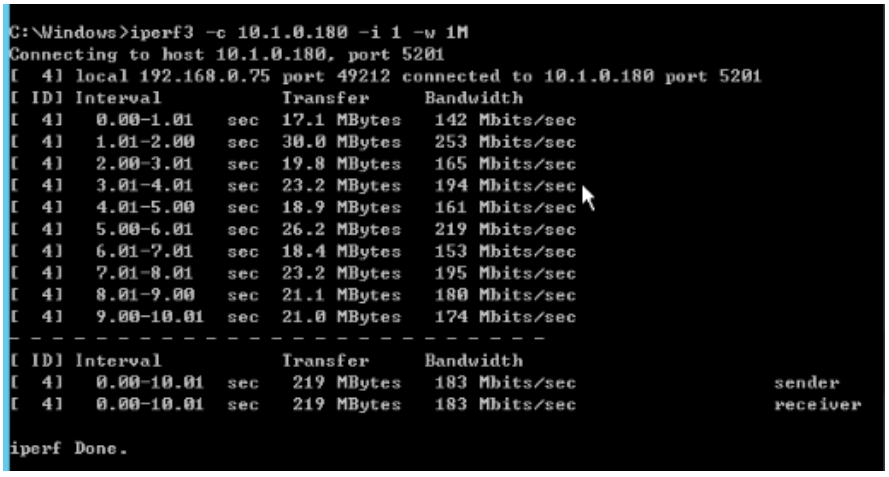
1. 互为对端的ECS都使用Windows系统，测试速率可达180Mbit/s，使用iperf3和filezilla（是一款支持ftp的文件传输工具）测试均满足带宽要求。

   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1-1所示。

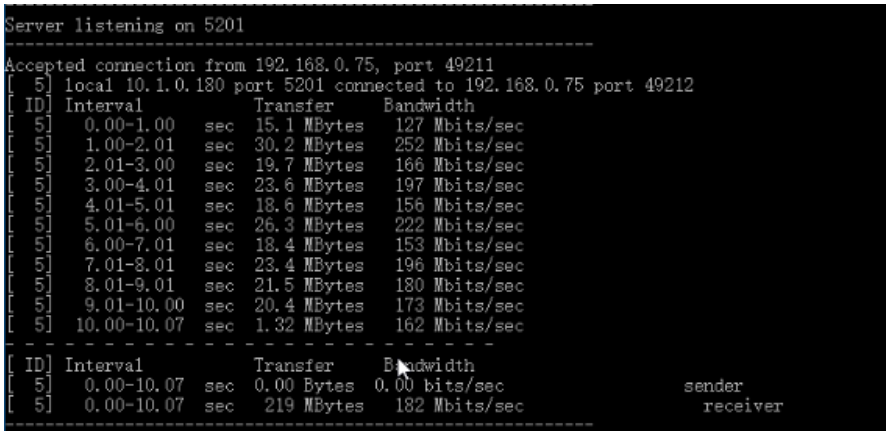
   图 1-1 200M 带宽客户端 iperf3 测试结果



使用iperf3服务器端测试结果截图如图1-2所示。

 版权所有 © 华为技术有限公司

图 1-2 200M 带宽服务端 iperf3 测试结果

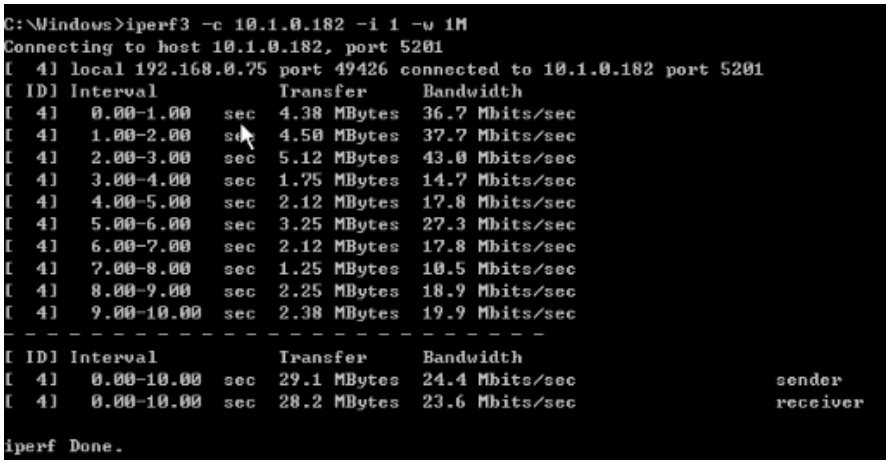


2. 互为对端的ECS都使用Centos7系统，测试速率可达180M，使用iperf3测试满足带宽要求。
3. 服务器端ECS使用Centos7系统，客户端使用Windows系统，测试速率只有20M左右，使用iperf3和filezilla测试均不能满足带宽要求。

   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1-3**所示。

图 1-3 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。具体ECS的规格可参见**ECS规格**。

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。

 版权所有 © 华为技术有限公司

1.1.15 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。

1.1.16 如何将按需的 VPN 转为包年/包月?

前提条件

- 计费方式选择为按带宽计费。即当前支持按带宽计费的按需计费方式转包年/包月。
- 按需按流量转包年/包月，需要先将按需按流量转为按需按带宽，再转包年/包月。

操作步骤

用户可以通过以下操作，在服务界面中将按带宽计费VPN网关转为包年/包月。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“VPN网关”界面目标VPN网关所在行，选择“更多>转包年/包月”。
6. 在“转包年/包月”弹窗界面，单击“确定”。

   说明

   包年/包月资源支持到期后续费降配，不可转按需。
7. 确认需要操作的VPN网关信息，选择续费时长，单击“去支付”。
8. 在支付界面，确认订单信息，选择优惠和付款方式，单击“确认付款”，完成支付。

   说明

   按需转包年/包月操作不会影响用户正常业务。

1.1.17 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。

 版权所有 © 华为技术有限公司

- 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。

1.1.18 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。

1.1.19 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。

1.1.20 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。

1.1.21 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）。

 版权所有 © 华为技术有限公司

1.1.22 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。

1.1.23 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；

1.1.24 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。

 版权所有 © 华为技术有限公司

1.1.25 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。

1.1.26 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。

1.1.27 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。

1.1.28 如何判断业务出云流量走哪个 EIP?

- 如果VPN网关的HA模式为主备模式。

  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。
- 如果VPN网关的HA模式为双活模式。
  - 关联模式为企业路由器：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。
  - 关联模式为虚拟私有云：对端子网和哪个EIP先创建VPN连接，则VPN网关到该对端子网的出云流量优先走该VPN连接。
- 用户可以通过以下操作，查看出云流量方向。

  a. 登录管理控制台。

  b. 在页面左上角单击  图标，选择区域，选择“管理与监督 > 云监控服务 CES”。

  c. 在左侧导航栏单击“云服务监控”，进入“云服务看板”。

  d. 在“云服务看板”界面，单击虚拟专用网络，进入“云服务看板详情”。

  e. 选择“企业版站点入云VPN连接”，单击“资源详情”，在目标VPN连接所在行的操作列，单击“查看监控指标”。

  此时可以看到VPN连接的监控指标， 若监控指标“发送速率”不为0，说明流量是从这条连接出。

1.2 产品咨询

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：

 版权所有 © 华为技术有限公司

  - 不同region之间创建VPN，实现跨region的VPC间网络互访。
  - 与其他公有云创建VPN，如与阿里云的VPC间网络互访。
  - 与客户IDC机房打通VPN，实现线上VPC与线下的IDC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。
  - 与家庭PPPoE拨号网络建立VPN连接。
  - 与4G/5G路由器建立VPN连接。
  - 与个人终端建立VPN连接。
- 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。

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。

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。

 版权所有 © 华为技术有限公司

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。

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。

请用户在购买包年/包月VPN网关时，根据规划连通的数据中心数量选择合适的VPN连接数。

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。

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。

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。

1.2.7 IPsec VPN 是否会自动建立连接？

支持自动建立连接。

版权所有 © 华为技术有限公司

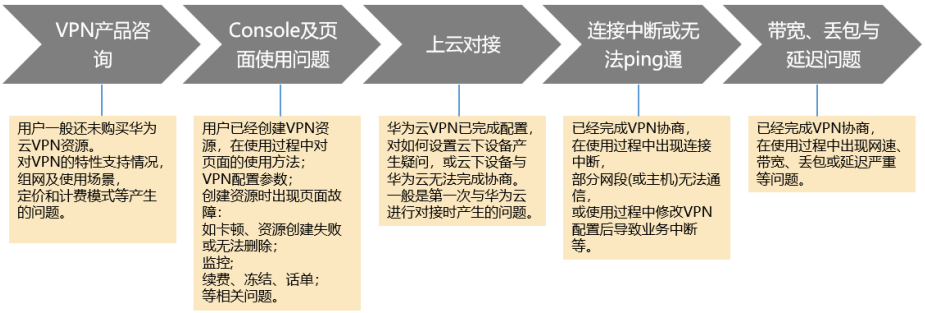
1.2.8 VPN 工单分类方法有哪些？如何提交 VPN 工单？

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。

说明

用户在**提交工单**时请选择相应的问题类型，有助于加速问题处理。

图 1-4 问题类型与分类依据



1.2.9 哪些设备可以与华为云进行 VPN 对接？

VPN支持标准IPsec协议，用户可以通过以下两个方面确认用户侧数据中心的设备能否与云进行对接：

1. 设备是否具备IPsec功能和授权：请查询设备的特性列表获取是否支持IPsec VPN。
2. 关于组网结构，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）也可以。

设备型号多为路由器、防火墙等，对接配置请参见**管理员指南**。

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。
- 与VPN服务做过对接测试厂商包括：
  - 设备厂商：华为（防火墙/AR）、山石（防火墙），CheckPoint（防火墙）。
  - 云服务厂商包括：阿里云，腾讯云，亚马逊（aws），微软（Microsoft Azure）。
  - 软件厂商包括：strongSwan。
- IPsec协议属于IETF标准协议，宣称支持该协议的厂商均可与云进行对接，用户不需要关注具体的设备型号。

  目前绝大多数企业级路由器和防火墙都支持该协议。
- 部分硬件厂商在特性规格列表中是宣称支持IPsec VPN的，但是需要专门购买软件License才能激活相关功能。

  请用户侧数据中心管理员根据设备具体型号与厂商进行确认。

版权所有 © 华为技术有限公司

1.2.10 VPN 协商参数有哪些？默认值是什么？

表 1-2 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
	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。

版权所有 © 华为技术有限公司

协议	配置项	值
	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
	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）

 版权所有 © 华为技术有限公司

协议	配置项	值
	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。
- 云侧不支持配置基于流量的IPsec SA生命周期，不会基于流量老化IPsec SA。

1.2.11 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。

1.2.12 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。

1.2.13 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。

 版权所有 © 华为技术有限公司

查询VPN网关监控状态，请在VPN网关“网关IP”列中单击EIP后面的 进行查看。

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。

查询VPN连接监控状态，请在VPN连接“监控”列中单击 进行查看。

1.2.14 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。

1.2.15 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。

1.2.16 虚拟专用网络是否支持 SSL VPN?

目前虚拟专用网络支持SSL VPN。

1.2.17 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。

1.2.18 VPN 是否支持 IPv6?

支持。

当前支持IPv4和IPv6的VPN网络。

1.2.19 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。

1.2.20 VPN 连接支持使用国产加密算法吗?

支持。

 版权所有 © 华为技术有限公司

请使用管理控制台界面提供的算法进行协商，请确保两端协商算法一致即可。

1.2.21 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。

 版权所有 © 华为技术有限公司

  - 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。

1.2.22 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1-3**所示。

表 1-3 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

 版权所有 © 华为技术有限公司

DH group	Modulus
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。

1.2.23 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）。

1.2.24 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。

1.2.25 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。

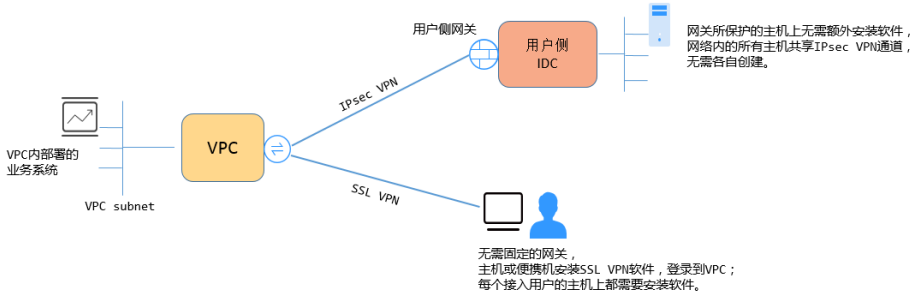
SSL VPN：连通的是一个客户端到一个局域网络，如出差员工的便携机访问公司内网。

版权所有 © 华为技术有限公司

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支持IPsec VPN和SSL VPN。

1.2.26 创建 VPN 都会产生哪些费用，VPN 网关 IP 收费吗?

VPN计费模式分为包年/包月和按需两种，费用包含：

- VPN网关费用
- VPN连接费用

  默认提供10条免费的VPN连接；超过10条后需要付费购买。
- VPN网关弹性公网IP带宽费用

  网关带宽的计费又可分为按流量或按带宽计费。

  a. 包年/包月计费模式下不可选择按流量计费。如果您选择包年/包月模式创建VPN，在创建网关阶段一次性收取网关带宽费用和连接的费用，用户后续创建VPN连接时不再收取费用。

  b. 按需方式为先使用后付费模式，计费周期为1小时。如果您选择按需模式创建VPN，页面会提示同时创建连接，费用包含了网关带宽费用和10个连接组费用，您在创建第11个连接组时只产生连接的费用。

  说明

  VPN网关的带宽费用是独立的，与ECS绑定的EIP带宽相互独立，无法共享。

1.2.27 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。

 版权所有 © 华为技术有限公司

如果选择包年/包月付费方式，则仅支持按带宽，不支持按流量；同时包年/包月付费方式相按需付费享受更多折扣优惠。

1.2.28 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。

1.2.29 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。

1.2.30 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。

1.2.31 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。

VPN连接状态请在VPN连接“监控”列中单击 进行查看。

1.2.32 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。

1.2.33 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：

 版权所有 © 华为技术有限公司

- 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。

1.2.34 VPN 网关或 VPN 连接误删后是否支持恢复?

- 包年/包月VPN网关或VPN连接不支持恢复。
- 按需VPN网关误删后支持恢复，但需要满足以下条件：
  - 按需VPN网关删除时长不能超过24小时；如果超过24小时则无法恢复。
  - 按需VPN网关删除时不能解绑EIP；如果VPN网关是在解绑任一EIP后再删除，则无法恢复。
  - 按需VPN网关对接的VPC或ER资源需要存在；如果不存在，请先恢复VPC或ER资源。
  - VPN网关对应的账户处于正常状态；如果账户处于欠费或冻结状态，则无法恢复。
- 按需VPN网关对应的VPN连接误删后支持恢复，但需要满足以下条件：
  - VPN连接对应的VPN网关和对端网关需要存在；如果不存在，请先恢复VPN网关和对端网关。
  - VPN网关对应的账户处于正常状态；如果账户处于欠费或冻结状态，则无法恢复。

  按需VPN连接恢复后，对应的健康检查项无法恢复，需要手动重新配置。

1.2.35 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。

- 基础型和专业型1 VPN网关规格，支持相互变更。
- 专业型1和专业型2 VPN网关规格，支持相互变更。
- 专业型1-非固定IP VPN网关规格不支持变更为专业型1；专业型2-非固定IP VPN网关规格不支持变更为专业型2；专业型3-非固定IP VPN网关规格不支持变更为专业型3。
- 仅“网络类型”为“公网”且“计费模式”采用“包年/包月”时，专业型1 VPN网关规格支持变更为专业型1-非固定IP；专业型2 VPN网关规格支持变更为专业型2-非固定IP；专业型3 VPN网关规格支持变更为专业型3-非固定IP。

1.2.36 经典版 VPN 是否支持升级企业版 VPN?

支持。

如果有升级需求，请**提交工单**进行申请。

1.2.37 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。

 版权所有 © 华为技术有限公司

1.3 组网与使用场景

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）。

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。

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。

 版权所有 © 华为技术有限公司

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

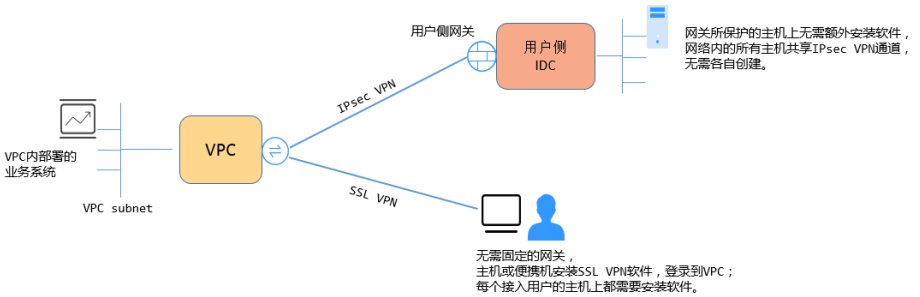
IPsec VPN：连通的是两个局域网，如分支机构与总部（或VPC）之间、本地IDC与云端VPC的子网；即IPsec VPN是网对网的连接。

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支持IPsec VPN和SSL VPN。

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。

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）。

 版权所有 © 华为技术有限公司

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
  - 购买VPN网关，配置计费模式、带宽大小和对接的VPC等信息。
  - 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。

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。

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。

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。

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）。

 版权所有 © 华为技术有限公司

- 如果两个VPC跨Region，请使用CC进行互联（需支付CC带宽费用）。

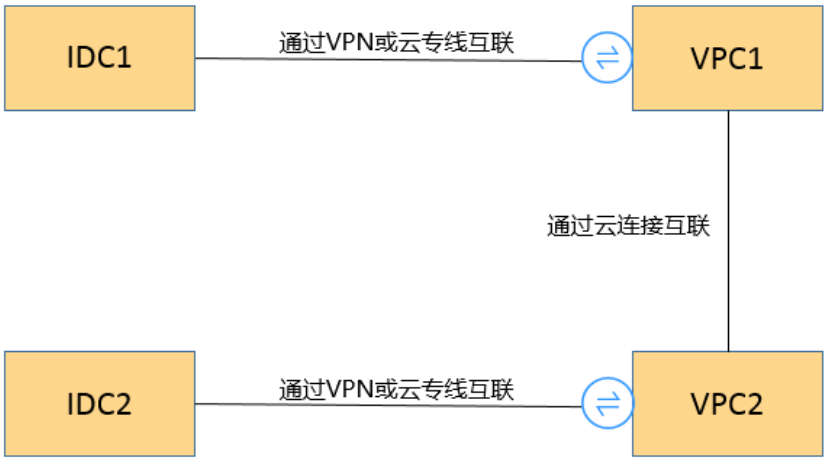
2. 用户侧数据中心IDC与其中一个VPC建立VPN连接。

   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。

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1-5所示。

图 1-5 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。

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。

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。

版权所有 © 华为技术有限公司

详细配置请参见**访问OBS**。

2. 在用户侧配置云的内网DNS和路由

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。

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。

1.3.17 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?

与云进行VPN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，对接指南详见**管理员指南**。

1.3.18 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。

1.4 计费类

1.4.1 创建 VPN 都会产生哪些费用，VPN 网关 IP 收费吗?

VPN提供包年/包月和按需计费两种计费模式，费用包含：

- VPN网关费用
- VPN连接费用

  默认提供10条免费的VPN连接；超过10条后需要付费购买。
- VPN网关弹性公网IP带宽费用

  网关带宽的计费又可分为按流量或按带宽计费。

版权所有 © 华为技术有限公司

a. 包年/包月计费模式下不可选择按流量计费。如果您选择包年/包月模式创建VPN，在创建网关阶段一次性收取网关带宽费用和连接的费用，用户后续创建VPN连接时不再收取费用。

b. 按需方式为先使用后付费模式，计费周期为1小时。如果您选择按需模式创建VPN，页面会提示同时创建连接，费用包含了网关带宽费用和10个连接组费用，您在创建第11个连接时组时只产生连接的费用。

说明

VPN网关的带宽费用是独立的，与ECS绑定的EIP带宽相互独立，无法共享。

1.4.2 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。

如果选择包年/包月付费方式，则仅支持按带宽，不支持按流量；同时包年/包月付费方式相按需付费享受更多折扣优惠。

1.4.3 按流量计费的 VPN 可以使用共享流量包?

企业版VPN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。

1.4.4 华为云的 Region 间创建的 VPN，按照几条连接计费?

使用VPN可以将不同Region间的VPC打通，每个Region的VPN带宽和VPN连接是独立的资源，独立计费。所以用户在预估费用时需要统计有几个Region，每个Region需要另外几个Region进行互通。

例如：Region A与Region B和C分别建立VPN连接，则Region A的VPN网关下有2条连接，分别与B、C连接；而Region B的VPN网关下有1条连接，Region C的VPN网关下有1条连接。

因此，用户整体在云上一共创建了4条VPN连接，只是每条连接都隶属于各自的Region。

1.4.5 如何将按需的 VPN 转为包年/包月?

操作步骤

用户可以通过以下操作，在服务界面中将按带宽计费VPN网关转为包年/包月。

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”。

 版权所有 © 华为技术有限公司

4. 在左侧导航栏选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“VPN网关”界面目标VPN网关所在行，选择“更多>转包年/包月”。
6. 在“转包年/包月”弹窗界面，单击“确定”。

   说明

   包年/包月资源支持到期后续费降配，不可转按需。
7. 确认需要操作的VPN网关信息，选择续费时长，单击“去支付”。
8. 在支付界面，确认订单信息，选择优惠和付款方式，单击“确认付款”，完成支付。

   说明

   按需转包年/包月操作不会影响用户正常业务。

1.4.6 包年/包月的 VPN 网关支持自动续费吗?

支持。

当前仅支持从预存费用中自动扣款续费。

当前包年/包月的收费模式为预付费，为确保您的连接正常使用，请提前为账户充值。

1.4.7 包年/包月的 VPN 网关支持退订吗?

支持。

在VPN网关列表页面，选择需要退订的网关，单击“更多”选项中的“退订”按钮。退订包年/包月VPN网关将同时删除该网关下创建的所有连接，且操作不可逆。

退订后包年/包月网关会退还剩余的预支付费用。

1.4.8 VPN 资源在什么情况下会被冻结，如何解除被冻结的 VPN 资源?

- 包年/包月的VPN资源在到期未续费时会进入宽限期，宽限期内您可正常访问及使用该资源。宽限期结束后，若您仍未续订，该资源将进入保留期，即被冻结状态。被冻结的资源不可用，也不能修改、删除。超过保留期仍未续费，冻结资源将被释放，被释放资源不可恢复。为确保资源持续可用，请在资源到期前及时续费。
- 按需的VPN资源在欠费时将资源置于欠费状态并进入宽限期，宽限期内您可正常访问及使用该资源。宽限期结束后，若您仍未缴清欠款，该资源将进入保留期，即被冻结状态。被冻结的资源不可用，也不能修改、删除。超过保留期仍未充值缴清欠费金额，冻结资源将被释放，被释放资源不可恢复。为确保资源持续可用，请在资源到期前完成充值，并确保所欠金额已结清。
- 共享带宽冻结时，EIP的行为以EIP资料为准。请参见**EIP资源在什么情况下会被冻结，如何解除被冻结的EIP资源?** 。
- 冻结的VPN资源在续费或充值后会变为可用状态。

1.4.9 VPN 资源如何扣费，如何使用优惠券?

VPN网关计费模式分为按需和包年/包月。

 版权所有 © 华为技术有限公司

- 按需为后付费，根据资源使用情况从账号余额中扣除费用。
- 包年/包月为预付费，创建资源时一次性扣除。

如果您已获得云优惠券，请在优惠券有效期内完成充值，充值后可按抵用资源使用费。

包年/包月资源在创建包年资源时会产生优惠费用，实际支付时费用可扣减。

合同用户需要在控制台页面选择“申请线上合同请款后支付”。

1.5 Console 与页面使用

1.5.1 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。

1.5.2 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。

1.5.3 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。

 版权所有 © 华为技术有限公司

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。

1.5.4 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。

1.5.5 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
    - 计费模式，包括包年/包月和按需计费
    - 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，请参见**EIP服务对应资料**。
    - 规格
      部分规格支持，以管理控制台界面为准。
    - VPN连接组数
      仅“计费模式”为“包年/包月”时需要设置。
  - 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

 版权所有 © 华为技术有限公司

        - 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
        - 策略规则
        - 预共享密钥
        - 分支互联
      - 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。
        - 检测机制
          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。

1.5.6 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。

1.5.7 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。

 版权所有 © 华为技术有限公司

1.5.8 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。

1.5.9 华为云是否支持 API?

支持。

1.5.10 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。

1.5.11 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。

1.5.12 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。

1.5.13 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）。

 版权所有 © 华为技术有限公司

1.5.14 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”。

1.5.15 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）；

如果页面长时间停留在删除或创建中，请**提交工单**解决。

1.5.16 VPN 网关最大支持多大带宽?

- 基础型网关规格最大支持100Mbps。
- 专业型1网关规格最大支持300Mbps。
- 专业型2网关规格最大支持1Gbps。
- 专业型3网关规格最大支持5Gbps。
- 国密型网关规格最大支持500Mbps。

1.5.17 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。

 版权所有 © 华为技术有限公司

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。

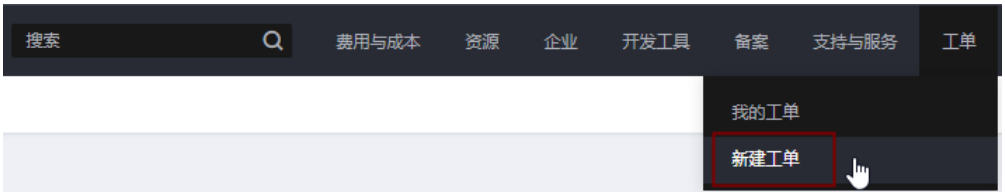
 版权所有 © 华为技术有限公司

- 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。

1.5.18 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”。

图 1-6 新建工单



3. 搜索并选择“VPN”。

图 1-7 选择工单产品分类

4. 选择问题类型。

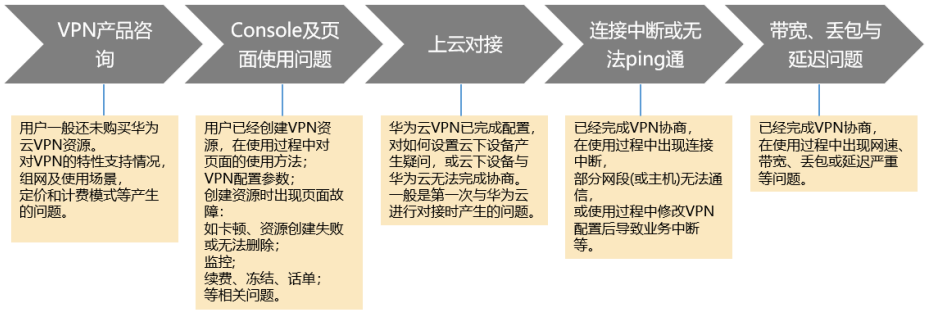
图 1-8 选择问题类型

 版权所有 © 华为技术有限公司

说明

用户在**提交工单**时请选择相应的问题类型，有助于加速问题处理。

图 1-9 问题类型与分类依据



1.5.19 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。

1.5.20 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。

查询VPN网关监控状态，请在VPN网关“网关IP”列中单击EIP后面的 进行查看。

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。

查询VPN连接监控状态，请在VPN连接“监控”列中单击 进行查看。

1.5.21 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。

版权所有 © 华为技术有限公司

VPN连接状态请在VPN连接“监控”列中单击 进行查看。

1.6 VPN 协商与对接

1.6.1 哪些设备可以与华为云进行 VPN 对接?

VPN支持标准IPsec协议，用户可以通过以下两个方面确认用户侧数据中心的设备能否与云进行对接：

1. 设备是否具备IPsec功能和授权：请查询设备的特性列表获取是否支持IPsec VPN。
2. 关于组网结构，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）也可以。

设备型号多为路由器、防火墙等，对接配置请参见**管理员指南**。

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。
- 与VPN服务做过对接测试厂商包括：
  - 设备厂商：华为（防火墙/AR）、山石（防火墙），CheckPoint（防火墙）。
  - 云服务厂商包括：阿里云，腾讯云，亚马逊（aws），微软（Microsoft Azure）。
  - 软件厂商包括：strongSwan。
- IPsec协议属于IETF标准协议，宣称支持该协议的厂商均可与云进行对接，用户不需要关注具体的设备型号。

  目前绝大多数企业级路由器和防火墙都支持该协议。
- 部分硬件厂商在特性规格列表中是宣称支持IPsec VPN的，但是需要专门购买软件License才能激活相关功能。

  请用户侧数据中心管理员根据设备具体型号与厂商进行确认。

1.6.2 VPN 协商参数有哪些? 默认值是什么?

表 1-4 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。

版权所有 © 华为技术有限公司

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。
	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。国密型VPN连接，只支持“v1”。） • 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。

版权所有 © 华为技术有限公司

协议	配置项	值
	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。
	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）

版权所有 © 华为技术有限公司

协议	配置项	值
	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。
- 云侧不支持配置基于流量的IPsec SA生命周期，不会基于流量老化IPsec SA。

1.6.3 IPsec VPN 是否会自动建立连接?

支持自动建立连接。

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

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

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

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

假设数据中心的子网为192.168.3.0/24和192.168.4.0/24，数据中心IPsec隧道的出口公网IP为1.1.1.2；VPC下的子网为192.168.1.0/24和192.168.2.0/24 ，VPC上IPsec隧道的出口公网IP为1.1.1.1。

操作步骤

1. 登录防火墙设备的命令行配置界面。
2. 查看防火墙版本信息。
   ```
   display version
   17:20:502017/03/09
   Huawei Versatile Security Platform Software
   Software Version: USG6600 V100R001C30SPC300(VRP (R) Software，Version 5.30)
   ```
3. 创建ACL。
   ```
   acl number 3065 vpn-instance vpn64
   rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   q
   ```
4. 创建ike proposal。
   ```
   ike proposal 64
   dh group5
   ```

 版权所有 © 华为技术有限公司

```
authentication-algorithm sha1
integrity-algorithm hmac-sha2-256
sa duration 3600
q
```

5. 创建ike peer，并引用之前创建的ike proposal，其中对端IP地址是1.1.1.1。

```
ike peer vpnikepeer_64
pre-shared-key ******** （********为您输入的预共享密码）
ike-proposal 64
undo version 2
remote-address vpn-instance vpn64 1.1.1.1
sa binding vpn-instance vpn64
q
```

6. 配置IPsec proposal。

```
IPsec proposal IPsecpro64
encapsulation-mode tunnel
esp authentication-algorithm sha1
q
```

7. 配置IPsec策略，并引用之前创建的IPsec proposal。

```
IPsec policy vpnIPsec64 1 isakmp
security acl 3065
pfs dh-group5
ike-peer vpnikepeer_64
proposal IPsecpro64
local-address 1.1.1.2
q
```

8. 将IPsec策略应用到相应的子接口上去。

```
interface GigabitEthernet0/0/2.64
IPsec policy vpnIPsec64
q
```

9. 测试连通性。

   在上述配置完成后，我们可以通过云上主机和数据中心的主机进行连通性测试，如下图图1-10所示。

图 1-10 连通性测试

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

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

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

 版权所有 © 华为技术有限公司

1.6.5 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。

1.6.6 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。

1.6.7 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。

1.6.8 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。

1.6.9 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。

 版权所有 © 华为技术有限公司

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。

1.6.10 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。

1.6.11 华为云对接 AWS 后，为何不可以从 AWS 向华为云发起协商?

VPN建立连接完成后，AWS为Response模式，并不主动发起协商，当从AWS的EC2向华为云ECS发起数据流时，也不触发该VPN建立SA。

按照AWS的知识文档，默认从客户侧（即对接AWS的云）发起被动协商，也支持修改为主动协商。

1.6.12 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。

1.6.13 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。

 版权所有 © 华为技术有限公司

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。

1.6.14 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。

1.6.15 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1-5所示。

表 1-5 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。

 版权所有 © 华为技术有限公司

1.7 连接故障或无法 PING 通

1.7.1 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。

1.7.2 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；

1.7.3 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。

 版权所有 © 华为技术有限公司

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。

如果执行以上操作均未触发IPsec隧道状态正常，请**提交工单**向云客服寻求帮助。

1.7.4 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

- 基础型网关规格最大支持100Mbps。
- 专业型1网关规格最大支持300Mbps。
- 专业型2网关规格最大支持1Gbps。
- 专业型3网关规格最大支持5Gbps。
- 国密型网关规格最大支持500Mbps。

1.7.5 IPsec VPN 是否会自动建立连接?

支持自动建立连接。

1.7.6 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。

1.7.7 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。

1.7.8 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。

 版权所有 © 华为技术有限公司

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。

1.7.9 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。

1.7.10 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。

1.7.11 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。

VPN连接状态请在VPN连接“监控”列中单击  进行查看。

1.7.12 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。

 版权所有 © 华为技术有限公司

1.7.13 VPN 建立后您的数据中心或局域网无法访问弹性云服务器?

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

1.7.14 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。

1.7.15 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。

1.8 公网地址

1.8.1 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。

1.8.2 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。

1.8.3 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。

1.8.4 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。

 版权所有 © 华为技术有限公司

1.8.5 用户侧数据中心的网关设备没有固定的公网 IP 可以吗?

可以。

用户数据中心与云进行VPN对接时，如果用户购买的VPN网关规格支持非固定IP接入能力，对端网关设备就可以使用非固定IP接入。

说明

VPN网关是否支持非固定IP接入能力，以管理控制台实际上线区域为准。

1.9 路由设置

1.9.1 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。

1.9.2 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。

1.9.3 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。

1.9.4 什么是 NQA

什么是 NQA

网络质量分析（Network Quality Analysis，NQA）是一种实时的网络性能探测和统计技术，可以对响应时间、网络抖动、丢包率等网络指标进行统计。NQA能够实时监视网络服务质量，在网络发生故障时进行有效的故障诊断和定位。

NQA 工作原理

图 1-11 NQA 客户端对 NQA 服务器端进行测试

 版权所有 © 华为技术有限公司

在NQA测试中，将发起NQA测试的源端称为NQA客户端，测试的目的端称为NQA服务器端。为使NQA客户端能够发起NQA测试，用户需要在NQA客户端中创建各类型的测试实例，构造符合相应协议的报文并打上时间戳，再发送至服务器端。

NQA服务器负责处理NQA客户端发来的测试报文，通过侦听指定IP地址和端口号的报文对客户端发起的测试进行响应。客户端根据发送和接收报文来计算各项性能指标，如连通性、时延、丢包率等。

NQA 测试例处理机制

ICMP测试是通过发送ICMP报文来判断目的地的可达性、计算网络响应时间及丢包率。

源端向目的端发送构造的ICMP Echo Request报文。目的端收到报文后，直接回应ICMP Echo Reply报文给源端。

源端收到报文后，通过计算源端接收时间和源端发送时间之差，计算出源端到目的端的通信时间，从而清晰地反映出网络性能及网络畅通情况。

NQA探测周期为10s，探测频率为10s内发3个ping请求。

为什么需要 NQA

随着运营商增值业务的开展，用户和运营商对QoS（Quality of Service）的相关要求越来越高，特别是在传统的IP网络承载语音和视频业务后，运营商与客户之间签订SLA（Service Level Agreement）成为普遍现象。

为了让用户看到承诺的带宽是否达到需求，运营商需要提供相关的时延、抖动、丢包率等相关的统计参数，以及时了解网络的性能状况。传统的网络性能分析方法（如Ping、Tracert等）已经不能满足用户对业务多样性和监测实时性的要求。NQA可以实现对网络运行状况的准确测试，输出统计信息。NQA可以监测网络上运行的多种协议的性能，使网络运营商能够实时采集到各种网络运行指标，例如：HTTP的总时延、TCP连接时延、DNS解析时延、文件传输速率、FTP连接时延、DNS解析错误率等。通过对这些指标进行控制，网络运营商可以为用户提供不同等级的网络服务。同时，NQA也是网络故障诊断和定位的有效工具。

静态路由与 NQA 联动

- 静态路由本身并没有检测机制，如果非本机直连链路发生了故障，静态路由不会自动从IP路由表中自动删除，需要网络管理员介入，这就无法保证及时进行链路切换，可能造成较长时间的业务中断。
- 使用静态路由模式创建VPN连接时，为了避免出现以上问题，需要使用NQA来检测静态路由所在的链路，确保VPN连接稳定性。使能NQA时需要确保对端网关设备支持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。
- 静态路由模式的VPN连接的使能NQA探测失败会撤销路由，需要对端网关放通从VPN连接本端隧道接口地址到对端隧道接口地址的ICMP协议流量。
- VPN连接的健康检查的NQA探测仅上报CES，失败无影响，需要对端网关放通从VPN网关公网IP到对端网关的公网IP的ICMP协议流量。

1.10 VPN 子网设置

 版权所有 © 华为技术有限公司

1.10.1 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）。

1.10.2 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

1.10.3 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。

1.10.4 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。

1.10.5 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。

1.10.6 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。

1.11 VPN 感兴趣流

 版权所有 © 华为技术有限公司

1.11.1 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。

1.11.2 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。

1.12 VPN 连接保活

1.12.1 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。

 版权所有 © 华为技术有限公司

1.13 监控类

1.13.1 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。

查询VPN网关监控状态，请在VPN网关“网关IP”列中单击EIP后面的 进行查看。

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。

查询VPN连接监控状态，请在VPN连接“监控”列中单击 进行查看。

1.13.2 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。

VPN连接状态请在VPN连接“监控”列中单击 进行查看。

1.13.3 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。

详细请参见**查看监控指标**。

1.13.4 当 VPN 监控结果异常时，可以发送提醒信息吗?

可以。

用户可以通过配置“消息通知服务”和 “云监控服务”实现VPN监控结果异常提醒。

1.14 带宽与网速

1.14.1 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。

 版权所有 © 华为技术有限公司

当用户购买的VPN网关的带宽为200Mbit/s时，测试情况如下。

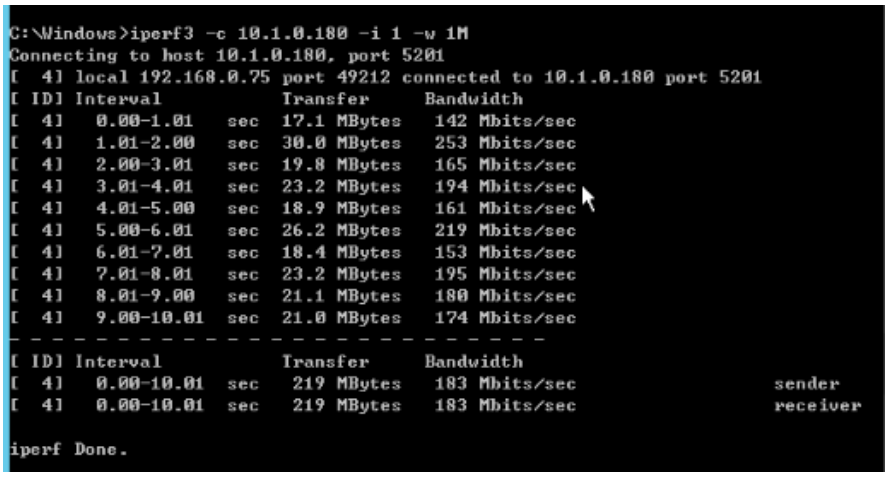
1. 互为对端的ECS都使用Windows系统，测试速率可达180Mbit/s，使用iperf3和filezilla（是一款支持ftp的文件传输工具）测试均满足带宽要求。

   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。

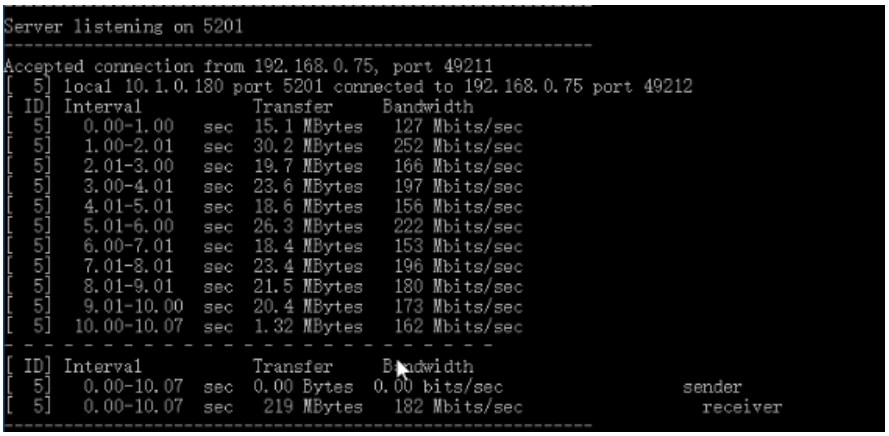
   使用iperf3客户端测试结果截图如图1-12所示。

   图 1-12 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1-13所示。

   图 1-13 200M 带宽服务端 iperf3 测试结果

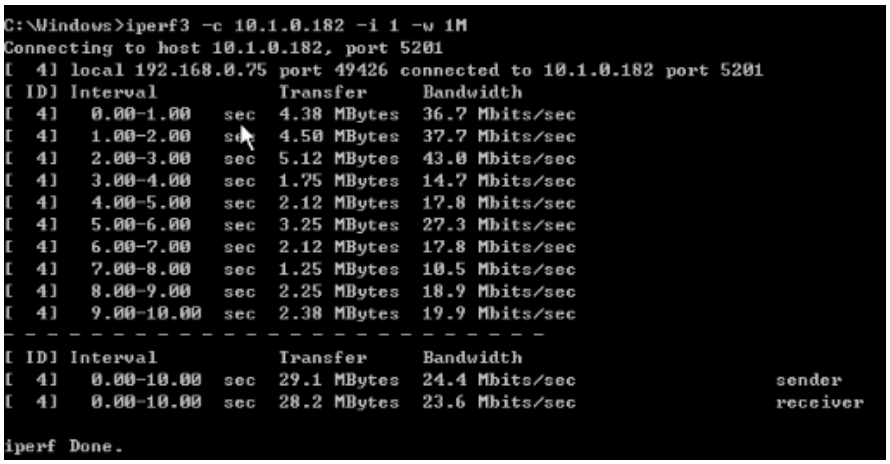
2. 互为对端的ECS都使用Centos7系统，测试速率可达180M，使用iperf3测试满足带宽要求。
3. 服务器端ECS使用Centos7系统，客户端使用Windows系统，测试速率只有20M左右，使用iperf3和filezilla测试均不能满足带宽要求。

   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1-14所示。

 版权所有 © 华为技术有限公司

图 1-14 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。

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。具体ECS的规格可参见**ECS规格**。

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。

1.14.2 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。

1.14.3 如何修改 VPN 的带宽大小?

1. 在VPN网关列表，单击目标VPN网关名称，进入网关详情页面。
2. 单击EIP带宽大小后的“修改”。
3. 配置EIP带宽信息。

   带宽修改以EIP的带宽修改规则为准，请参见**修改EIP的带宽配置**。

说明

EIP的带宽不能超过VPN的规格带宽。

 版权所有 © 华为技术有限公司

1.14.4 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

- 基础型网关规格最大支持100Mbps。
- 专业型1网关规格最大支持300Mbps。
- 专业型2网关规格最大支持1Gbps。
- 专业型3网关规格最大支持5Gbps。
- 国密型网关规格最大支持500Mbps。

1.14.5 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。

1.14.6 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，详细请参见**VPN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支持的最大带宽如下：
  - 基础型网关规格最大支持100Mbps。
  - 专业型1网关规格最大支持300Mbps。
  - 专业型2网关规格最大支持1Gbps。
  - 专业型3网关规格最大支持5Gbps。
  - 国密型网关规格最大支持500Mbps。

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。

 版权所有 © 华为技术有限公司

1.14.7 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。

1.15 配额类

1.15.1 虚拟专用网络的配额是什么?

什么是配额?

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少台弹性云服务器、多少块云硬盘。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

资源类型

VPN的资源类型包括VPN网关、VPN连接和对端网关，对应资源类型的总配额根据部署Region存在差异，请以实际部署环境为准。

怎样查看我的配额?

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

如何申请扩大配额?

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

1.15.2 创建 VPN 网关和连接的缺省配额是多少?

每个用户缺省可创建50个VPN网关和100个对端网关；每个VPN网关缺省可创建100个连接组。其中，VPN网关不同EIP对接到对端网关的同一个公网IP占用1个VPN连接组配额；VPN网关不同EIP对接到对端网关的不同公网IP或多个对端网关的公网IP占用2个VPN连接组配额。

 版权所有 © 华为技术有限公司

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

1.15.3 如何修改当前客户的 VPN 网关和连接的配额?

1. 进入管理控制台，在界面右上方选择“工单管理 > 新建工单 ”
2. 选择问题所属产品：选择“业务类 > 配额类”。
3. 选择问题类型：单击“配额申请”。
4. 新建工单：单击“新建工单”。
   填写区域、问题描述等信息，单击“提交”。

1.15.4 一个用户下支持多少个 IPsec VPN?

每个用户缺省可创建50个VPN网关和100个对端网关；每个VPN网关缺省可创建100个连接组。其中，VPN网关不同EIP对接到对端网关的同一个公网IP占用1个VPN连接组配额；VPN网关不同EIP对接到对端网关的不同公网IP或多个对端网关的公网IP占用2个VPN连接组配额。

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

1.16 账号权限

1.16.1 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。

1.16.2 创建 VPN 时系统提示权限不足，如何处理?

- 确认您的账号为子账号。
- 确保子账号具有“VPN FullAccess”权限。详细操作请参见**创建用户组并授权**和**用户组添加用户**。

1.16.3 如何确定我的账号是因为权限不足而无法创建 VPN 的?

创建VPN网关或连接时提示权限不足，请添加对应的权限。

账号创建VPN所需权限详见**基于IAM进行权限管理**。

 版权所有 © 华为技术有限公司

2 站点入云 VPN 经典版

2.1 热点问题

2.1.1 哪些设备可以与云进行 VPN 对接?

VPN支持标准IPsec协议，用户可以通过以下两个方面确认用户侧数据中心的设备能否与云进行对接：

1. 设备是否具备IPsec功能和授权：请查询设备的特性列表获取是否支持IPsec VPN。
2. 关于组网结构，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）也可以。

设备型号多为路由器、防火墙等，对接配置请参见**管理员指南**。

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。
- 与VPN服务做过对接测试厂商包括但不限于：华为（路由器、防火墙）、h3c（路由器、防火墙）、cisco（路由器、防火墙）、锐捷（路由器、防火墙）、中兴、深信服、fortinet、360、天融信、山石、网康、绿盟、DELL、合勤、Juniper等。
- 云服务厂商包括但不限于：阿里云，腾讯云，亚马逊（aws）。
- 软件厂商包括但不限于：Openswan/strongSwan、GreenBow等 。
- IPsec协议属于IETF标准协议，宣称支持该协议的厂商均可与云进行对接，用户不需要关注具体的设备型号。

  目前绝大多数企业级路由器和防火墙都支持该协议。
- 部分硬件厂商在特性规格列表中是宣称支持IPsec VPN的，但是需要专门购买软件License才能激活相关功能。

  请用户侧数据中心管理员根据设备具体型号与厂商进行确认。

 版权所有 © 华为技术有限公司

2.1.2 VPN 协商参数有哪些？默认值是什么？

表 2-1 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-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

版权所有 © 华为技术有限公司

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）
	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。

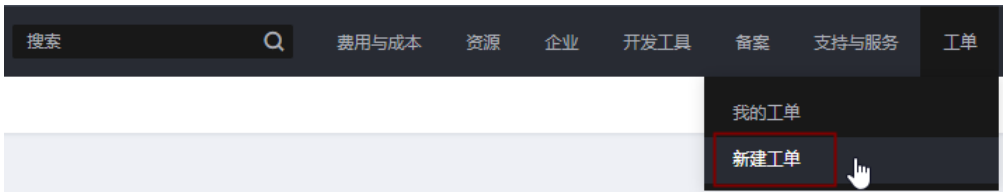
  IKE协商分为两个阶段，第二阶段（IPsec SA）的密钥都是由第一阶段协商生成的密钥衍生的，一旦第一阶段的密钥泄露将可能导致IPsec VPN受到侵犯。为提升密钥管理的安全性，IKE提供了PFS（完美向前保密）功能。启用PFS后，在进行IPsec SA协商时会进行一次附加的DH交换，重新生成新的IPsec SA密钥，提高了IPsec SA的安全性。
- 为了增强安全性，云默认开启PFS，请用户在配置用户侧数据中心网关设备时确认也开启了该功能，否则会导致协商失败。
- 用户开启此功能的同时，需要保证两端配置一致。
- IPsec SA字节生命周期，不是VPN服务可配置参数，云侧采用的是默认配置1843200KB。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

 版权所有 © 华为技术有限公司

2.1.3 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”。

图 2-1 新建工单



3. 搜索并选择“VPN”。

图 2-2 选择工单产品分类

4. 选择问题类型。

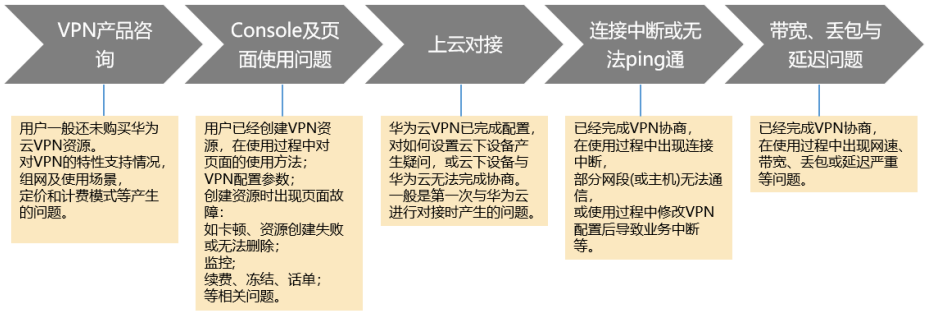
图 2-3 选择问题类型

 版权所有 © 华为技术有限公司

说明

用户在**提交工单**时请选择相应的问题类型，有助于加速问题处理。

图 2-4 问题类型与分类依据



2.1.4 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。

2.1.5 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）。

2.1.6 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）和远端子网（用户侧子网）， 无需配置多个连接。

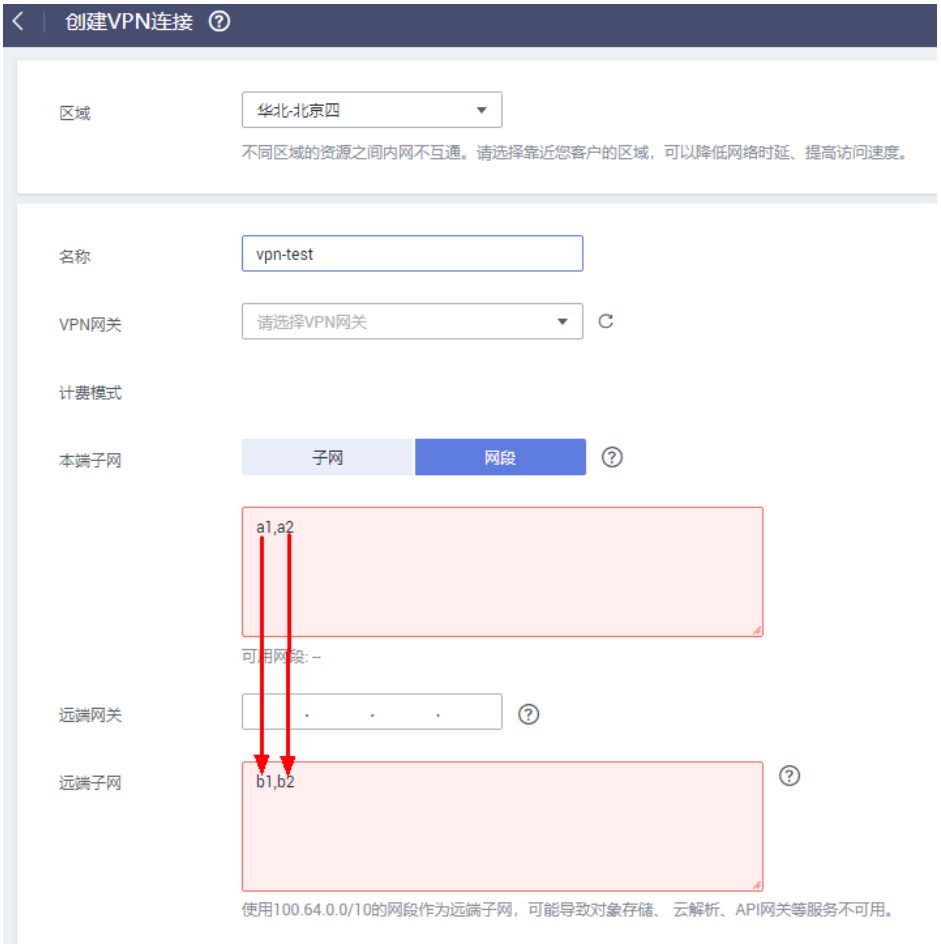
拟创建VPN连接的数量通常与用户数据中心数量有关，每条VPN连接可打通当前VPC与云下的一个数据中心网络。

请用户在购买包年/包月VPN网关时，根据规划连通的数据中心数量选择合适的VPN连接数。

版权所有 © 华为技术有限公司

说明

例如，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，在该连接中指定云侧多个源网段和多个地址网段即可。如下图所示：



2.1.7 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。

2.1.8 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。

版权所有 © 华为技术有限公司

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。

2.1.9 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

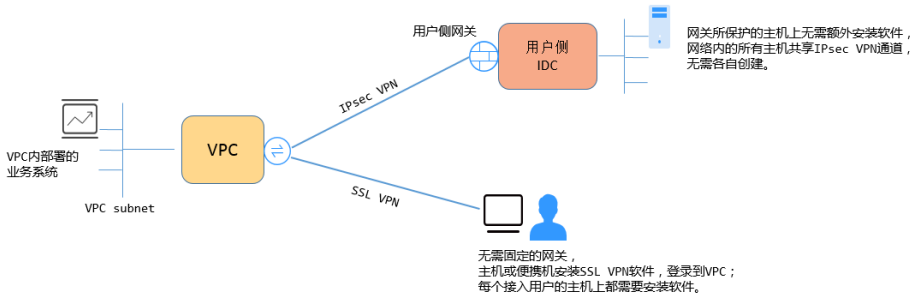
IPsec VPN连通的是两个局域网，如分支机构与总部（或VPC）之间、本地IDC与云端VPC的子网，即IPsec VPN是网对网的连接。

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支持IPsec VPN和SSL VPN。

2.1.10 IPsec VPN 是否会自动建立连接?

IPsec VPN在完成两侧配置后，并不会自行建立连接，需要两侧主机间的数据流来触发隧道的建立。如果云上与用户侧数据中心没有交互数据流，VPN的连接状态会一直处于Down状态。所谓的数据流，可以是真实的业务访问数据，也可以是主机间Ping测数据。

触发隧道建立的方式有两种，一种是通过建立连接间的网关设备自动触发协商，另一种是通过云上云下主机间的交互流量触发。

暂不支持通过云端VPN网关自动触发协商。推荐您在首次建立连接时，分别验证两侧的交互数据流均可触发连接建立。即用户侧数据中心主机ping云上主机可触发连接建立，然后断开连接，确认云上主机Ping用户侧数据中心主机亦可触发连接建立。

版权所有 © 华为技术有限公司

说明

Ping包的源地址、目的地址需要处于VPN保护的范围内。

在建立连接之前，两端的网关地址应该是可以Ping通的，但是Ping网关IP并不触发VPN连接的建立。

2.1.11 创建 VPN 都会产生哪些费用，VPN 网关 IP 收费吗?

VPN提供包年/包月和按需两种计费模式，费用包含网关带宽费用和VPN连接费用。计费模式以实际region购买界面为准。

网关带宽的计费又可分为按流量或按带宽计费。

1. 包年/包月计费模式下不可选择按流量计费。如果您选择包年/包月模式创建VPN，在创建网关阶段一次性收取网关带宽费用和连接的费用，用户后续创建VPN连接时不再收取费用。
2. 按需方式为先使用后付费模式，计费周期为1小时。如果您选择按需模式创建VPN，页面会提示同时创建连接。费用包含了网关带宽费用和单条连接费用，您在创建第二条连接时只产生连接的费用。

说明

- VPN网关IP不收费，只收取VPN网关的带宽费用。
- VPN网关的带宽费用是独立的，与ECS绑定的EIP带宽相互独立，无法共享。

2.1.12 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。

2.1.13 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”。

2.1.14 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：

 版权所有 © 华为技术有限公司

- 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。

2.1.15 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2-5所示。

图 2-5 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2-6所示。

图 2-6 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
-----------------------------------------------------------
```

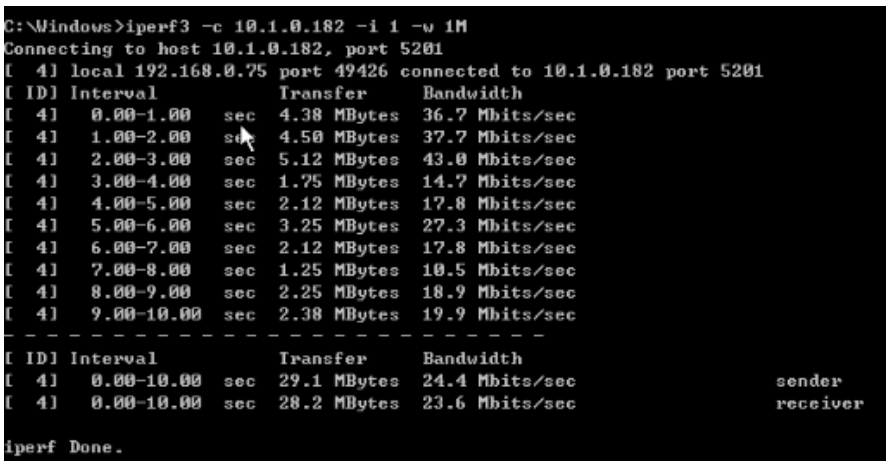
 版权所有 © 华为技术有限公司

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2-7**所示。

   图 2-7 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。具体ECS的规格可参见**ECS规格**。

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。

2.1.16 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。

2.1.17 如何将按需的 VPN 转为包年/包月

前提条件

- 计费方式选择为按带宽计费。即当前支持按带宽计费的按需计费方式转包年/包月。

  按需按流量转包年/包月，需要先将按需按流量转为按需按带宽，再转包年/包月。
- 已创建的VPN连接数量小于10个。
- 账号下可创建VPN连接的配额余量不少于10个。

操作步骤

用户可以通过以下操作，在服务界面中将按带宽计费VPN网关转为包年/包月。

 版权所有 © 华为技术有限公司

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > 经典版”。
5. 在“VPN网关”界面目标VPN网关所在行，选择“更多>转包年/包月”。
6. 在“转包年/包月”弹窗界面，单击“确定”。

   说明

   - 包年/包月资源不支持转按需。
   - 包年/包月资源支持到期后续费降配。
   - 包年/包月模式下，VPN连接数表示基于当前VPN网关可免费创建的VPN连接的数量。
   - 按需转包年/包月场景下，按需VPN网关只能转为VPN连接数为10个的包年/包月VPN网关。
7. 在“按需转包年/包月”界面，确认需要操作的VPN网关信息，选择续费时长。

   单击“去支付”。
8. 在支付界面，确认订单信息，选择优惠和付款方式。

   单击“确认付款”，完成支付。

   说明

   按需转包年/包月操作不会影响用户正常业务。

2.1.18 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。

 版权所有 © 华为技术有限公司

2.1.19 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。

2.1.20 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。

2.1.21 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。

2.1.22 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。

2.1.23 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。

 版权所有 © 华为技术有限公司

2.1.24 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；
- 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 &
```

 版权所有 © 华为技术有限公司

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. 使用文件执行以下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。

2.1.25 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。

2.1.26 如何解决 VPN 连接无法建立连接问题?

1. 检查云上VPN连接中的IKE策略和IPsec策略中的协商模式和加密算法是否与远端配置一致。
   a. 如果第一阶段IKE策略已经建立，第二阶段的IPsec策略未开启，常见情况为IPsec策略与数据中心远端的配置不一致。
   b. 如果客户本地侧使用的是CISCO的物理设备，建议客户使用MD5算法。同时将云上VPN连接端IPsec策略中的认证算法设置为MD5。
2. 检查ACL是否配置正确。
   假设您的数据中心的子网为192.168.3.0/24和192.168.4.0/24，VPC下的子网为192.168.1.0/24和192.168.2.0/24，则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。

2.1.27 EIP 能作为 VPN 的网关 IP 吗?

企业版VPN可以；经典版VPN不可以。

2.1.28 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。

 版权所有 © 华为技术有限公司

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。

2.1.29 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2-2所示。

表 2-2 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

其他满足参考标准和协议的设备，也在支持列表中，但是可能会因为设备对协议的实现方式不一致，导致接入失败。

2.1.30 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。

2.2 产品咨询

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。
  - 华为云与友商云创建VPN，如与阿里云的VPC间网络互访。
  - 华为云与客户IDC机房打通VPN，实现线上VPC与线下的IDC网络互访。

 版权所有 © 华为技术有限公司

  - 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。
  - 与家庭PPPoE拨号网络建立VPN连接。
  - 与4G/5G路由器建立VPN连接。
  - 与个人终端建立VPN连接。
- 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。

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。

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。

 版权所有 © 华为技术有限公司

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

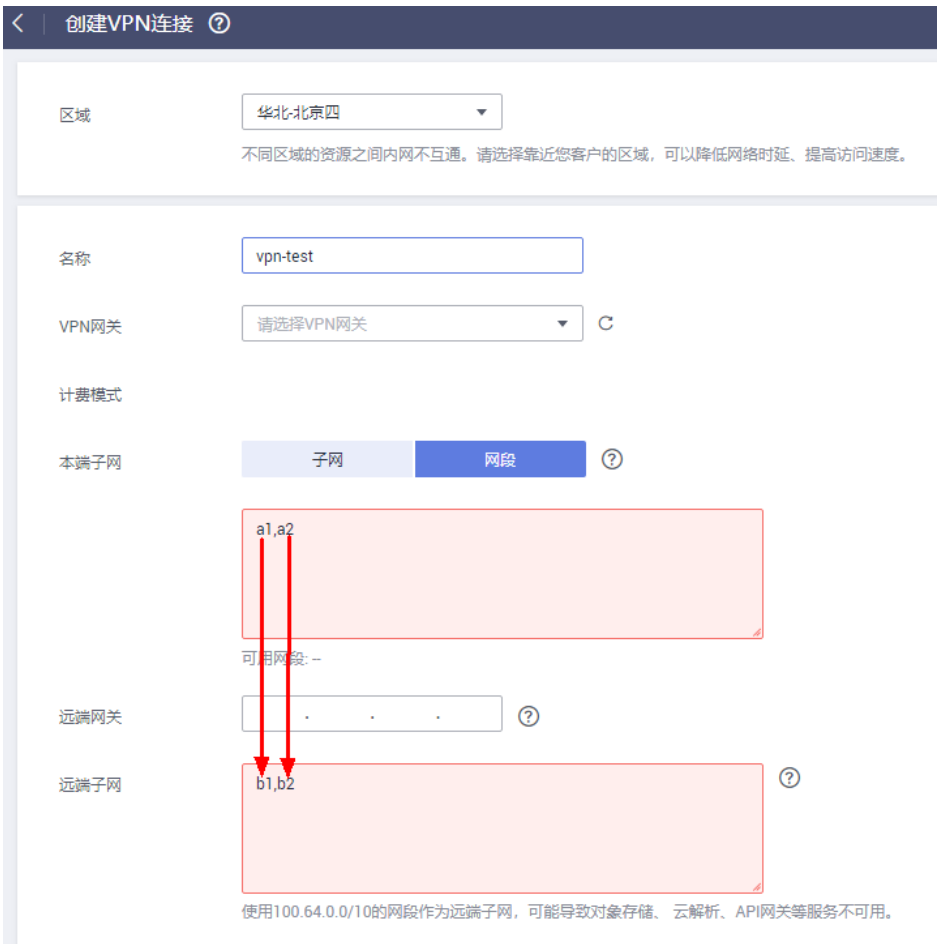
VPN连接，指华为云的一个VPN网关与用户侧一个独立的公网IP之间建立的IPsec连接，一个连接中可以配置多个本端子网（vpc中的子网）和远端子网（用户侧子网），无需配置多个连接。

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。

请用户在购买包年/包月VPN网关时，根据规划连通的数据中心数量选择合适的VPN连接数。

说明

例如，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，在该连接中指定云侧多个源网段和多个地址网段即可。如下图所示：



 版权所有 © 华为技术有限公司

2.2.5 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。

2.2.6 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。

2.2.7 IPsec VPN 是否会自动建立连接?

IPsec VPN在完成两侧配置后，并不会自行建立连接，需要两侧主机间的数据流来触发隧道的建立。如果云上与用户侧数据中心间没有交互数据流，VPN的连接状态会一直处于Down状态。所谓的数据流，可以是真实的业务访问数据，也可以是主机间Ping测数据。

触发隧道建立的方式有两种，一种是通过建立连接间的网关设备自动触发协商，另一种是通过云上云下主机间的交互流量触发。

暂不支持通过云端VPN网关自动触发协商。推荐您在首次建立连接时，分别验证两侧的交互数据流均可触发连接建立。即用户侧数据中心主机ping云上主机可触发连接建立，然后断开连接，确认云上主机Ping用户侧数据中心主机亦可触发连接建立。

说明

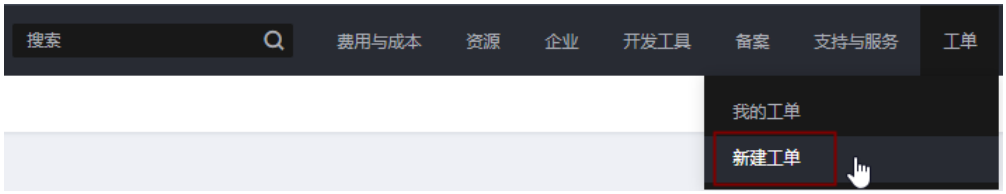
Ping包的源地址、目的地址需要处于VPN保护的范围内。

在建立连接之前，两端的网关地址应该是可以Ping通的，但是Ping网关IP并不触发VPN连接的建立。

2.2.8 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”。

图 2-8 新建工单



3. 搜索并选择“VPN”。

 版权所有 © 华为技术有限公司

图 2-9 选择工单产品分类

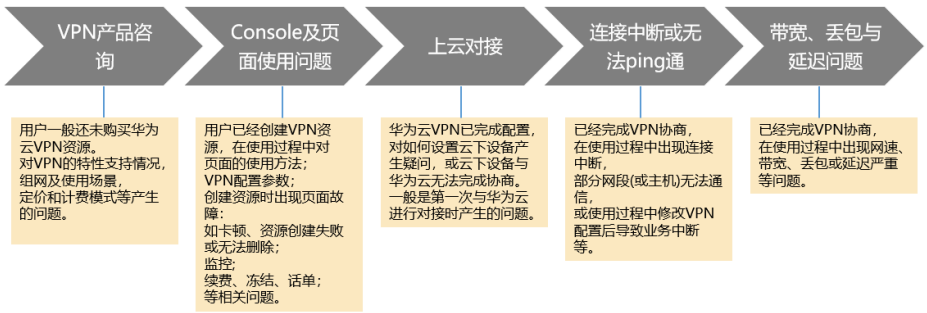
4. 选择问题类型。

图 2-10 选择问题类型

说明

用户在**提交工单**时请选择相应的问题类型，有助于加速问题处理。

图 2-11 问题类型与分类依据



 版权所有 © 华为技术有限公司

2.2.9 VPN 协商参数有哪些？默认值是什么？

表 2-3 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。
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

 版权所有 © 华为技术有限公司

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）
	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。

 版权所有 © 华为技术有限公司

2.2.10 哪些设备可以与云进行 VPN 对接?

VPN支持标准IPsec协议，用户可以通过以下两个方面确认用户侧数据中心的设备能否与云进行对接：

1. 设备是否具备IPsec功能和授权：请查询设备的特性列表获取是否支持IPsec VPN。
2. 关于组网结构，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）也可以。

设备型号多为路由器、防火墙等，对接配置请参见**管理员指南**。

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进行对接。
- 与VPN服务做过对接测试厂商包括：
  - 设备厂商：华为（防火墙/AR）、山石（防火墙），CheckPoint（防火墙）。
  - 云服务厂商包括：阿里云，腾讯云，亚马逊（aws），微软（Microsoft Azure）。
  - 软件厂商包括：strongSwan。
- IPsec协议属于IETF标准协议，宣称支持该协议的厂商均可与云进行对接，用户不需要关注具体的设备型号。

  目前绝大多数企业级路由器和防火墙都支持该协议。
- 部分硬件厂商在特性规格列表中是宣称支持IPsec VPN的，但是需要专门购买软件License才能激活相关功能。

  请用户侧数据中心管理员根据设备具体型号与厂商进行确认。

2.2.11 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。

2.2.12 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

 版权所有 © 华为技术有限公司

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。

2.2.13 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”。

2.2.14 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。

2.2.15 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。

2.2.16 虚拟专用网络是否支持 SSL VPN?

目前虚拟专用网络支持SSL VPN。

2.2.17 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。

2.2.18 无带宽信息的网关无法创建新的连接如何解决?

经典版VPN网关无带宽显示，说明该网关为老版VPN的产品，云已不支持创建该版本的产品。

- 老版VPN在使用过程中带宽无法保障，一个网关只能创建一条连接，用户可以删除网关后重建（影响业务）；
- 默认情况下变更至新版VPN网关的带宽规格为10M，用户后期可根据实际需要调整带宽大小； 变更后转为包年/包月的网关支持到期后续费带宽降配。

2.2.19 VPN 是否支持 IPv6?

不支持。

 版权所有 © 华为技术有限公司

当前云只支持IPv4。

2.2.20 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。

2.2.21 VPN 连接支持使用国产加密算法吗?

不支持。

请使用管理控制台界面提供的算法进行协商，请确保两端协商算法一致即可。

2.2.22 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

 版权所有 © 华为技术有限公司

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。

2.2.23 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2-4**所示。

 版权所有 © 华为技术有限公司

表 2-4 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。

2.2.24 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）。

2.2.25 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。

 版权所有 © 华为技术有限公司

2.2.26 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

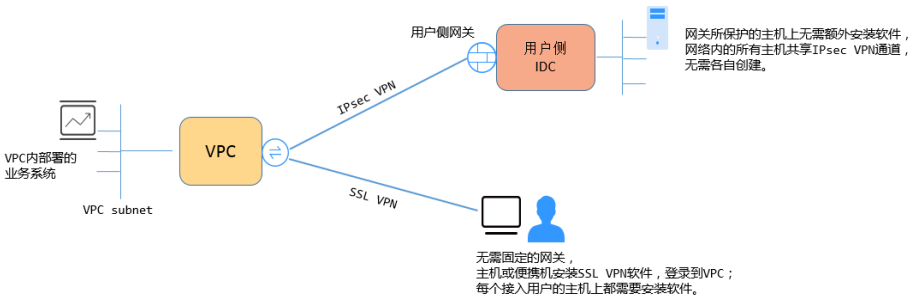
IPsec VPN：连通的是两个局域网，如分支机构与总部（或VPC）之间、本地IDC与云端VPC的子网；即IPsec VPN是网对网的连接。

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支持IPsec VPN和SSL VPN。

2.2.27 创建 VPN 都会产生哪些费用，VPN 网关 IP 收费吗?

VPN计费模式分为包年/包月和按需两种，费用包含网关带宽费用和VPN连接费用。计费模式以实际region购买界面为准。

网关带宽的计费又可分为按流量或按带宽计费。

1. 包年/包月计费模式下不可选择按流量计费。如果您选择包年/包月模式创建VPN，在创建网关阶段一次性收取网关带宽费用和连接的费用，用户后续创建VPN连接时不再收取费用。
2. 按需方式为先使用后付费模式，计费周期为1小时。如果您选择按需模式创建VPN，页面会提示同时创建连接。费用包含了网关带宽费用和单条连接费用，您在创建第二条连接时只产生连接的费用。

   说明

   - VPN网关IP不收费，只收取VPN网关的带宽费用。
   - VPN网关的带宽费用是独立的，与ECS绑定的EIP带宽相互独立，无法共享。

版权所有 © 华为技术有限公司

2.2.28 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。

如果选择包年/包月付费方式，则仅支持按带宽，不支持按流量；同时包年/包月付费方式相按需付费享受更多折扣优惠。

2.2.29 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。

2.2.30 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。

2.2.31 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。

2.2.32 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。

2.2.33 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。

 版权所有 © 华为技术有限公司

2.2.34 如何解决 VPN 连接无法建立连接问题?

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

   假设您的数据中心的子网为192.168.3.0/24和192.168.4.0/24，VPC下的子网为192.168.1.0/24和192.168.2.0/24，则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。

2.2.35 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。

2.3 组网与使用场景

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）。

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。

 版权所有 © 华为技术有限公司

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。

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。

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。

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。

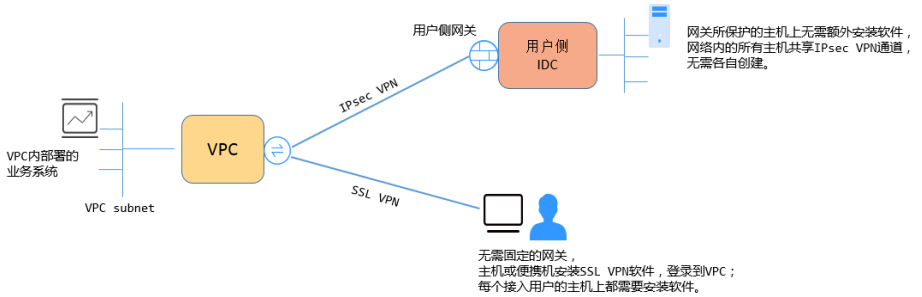
SSL VPN：连通的是一个客户端到一个局域网络，如出差员工的便携机访问公司内网。

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。

 版权所有 © 华为技术有限公司



说明

VPN支持IPsec VPN和SSL VPN。

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。

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。

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。

 版权所有 © 华为技术有限公司

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。

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。

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。

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。

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。

版权所有 © 华为技术有限公司

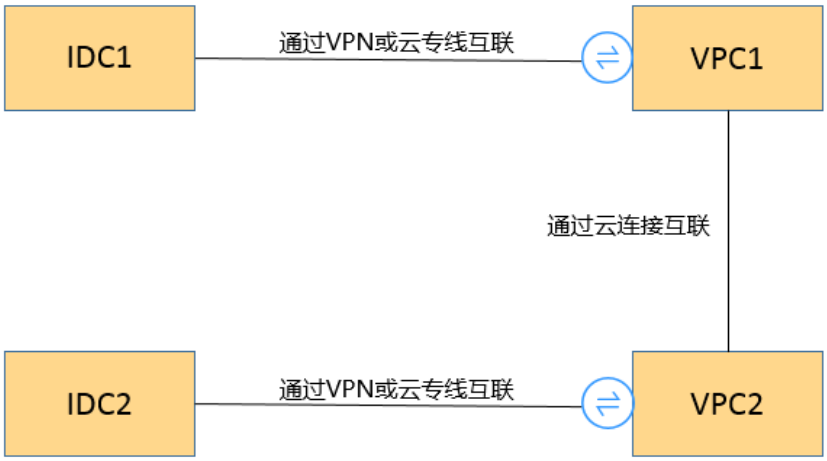
配置步骤

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。

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2-12所示。

图 2-12 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。

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。

 版权所有 © 华为技术有限公司

2.3.16 VPN 和 OBS 可以直接通信吗?

可以。

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。

然后在用户侧配置云的内网DNS和路由。

详细配置请参见**访问OBS**。

2.3.17 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。

2.3.18 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。

2.3.19 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，对接指南详见**管理员指南**。

2.3.20 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。

2.4 计费类

2.4.1 创建 VPN 都会产生哪些费用，VPN 网关 IP 收费吗?

VPN提供包年/包月和按需计费两种计费模式，费用包含网关带宽费用和VPN连接费用。计费模式以实际region购买界面为准。

 版权所有 © 华为技术有限公司

网关带宽的计费又可分为按流量或按带宽计费。

1. 包年/包月计费模式下不可选择按流量计费。如果您选择包年/包月模式创建VPN，在创建网关阶段一次性收取网关带宽费用和连接的费用，用户后续创建VPN连接时不再收取费用。
2. 按需方式为先使用后付费模式，计费周期为1小时。如果您选择按需模式创建VPN，页面会提示同时创建连接。费用包含了网关带宽费用和单条连接费用，您在创建第二条连接时只产生连接的费用。

说明

- VPN网关IP不收费，只收取VPN网关的带宽费用。
- VPN网关的带宽费用是独立的，与ECS绑定的EIP带宽相互独立，无法共享。

2.4.2 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。

如果选择包年/包月付费方式，则仅支持按带宽，不支持按流量；同时包年/包月付费方式相按需付费享受更多折扣优惠。

2.4.3 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。

2.4.4 华为云的 Region 间创建的 VPN，按照几条连接计费?

使用VPN可以将不同Region间的VPC打通，每个Region的VPN带宽和VPN连接是独立的资源，独立计费。所以用户在预估费用时需要统计有几个Region，每个Region需要另外几个Region进行互通。

例如：Region A与Region B和C分别建立VPN连接，则Region A的VPN网关下有2条连接，分别与B、C连接；而Region B的VPN网关下有1条连接，Region C的VPN网关下有1条连接。

因此，用户整体在云上一共创建了4条VPN连接，只是每条连接都隶属于各自的Region。

2.4.5 如何将按需的 VPN 转为包年/包月?

前提条件

- 计费方式选择为按带宽计费。即当前支持按带宽计费的按需计费方式转包年/包月。

  按需按流量转包年/包月，需要先将按需按流量转为按需按带宽，再转包年/包月。

 版权所有 © 华为技术有限公司

- 已创建的VPN连接数量小于10个。
- 账号下可创建VPN连接的配额余量不少于10个。

操作步骤

用户可以通过以下操作，在服务界面中将按带宽计费VPN网关转为包年/包月。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > 经典版”。
5. 在“VPN网关”界面目标VPN网关所在行，选择“更多>转包年/包月”。
6. 在“转包年/包月”弹窗界面，单击“确定”。

   说明

   - 包年/包月资源不支持转按需。
   - 包年/包月资源支持到期后续费降配。
   - 包年/包月模式下，VPN连接数表示基于当前VPN网关可免费创建的VPN连接的数量。
   - 按需转包年/包月场景下，按需VPN网关只能转为VPN连接数为10个的包年/包月VPN网关。
7. 在“按需转包年/包月”界面，确认需要操作的VPN网关信息，选择续费时长。
   单击“去支付”。
8. 在支付界面，确认订单信息，选择优惠和付款方式。
   单击“确认付款”，完成支付。

   说明

   按需转包年/包月操作不会影响用户正常业务。

2.4.6 包年/包月的 VPN 网关支持自动续费吗?

支持。

云当前仅支持从预存费用中自动扣款续费。

当前包年/包月为收费模式为预付费，为确保您的连接正常使用，请提前为账户充值。

2.4.7 包年/包月的 VPN 网关支持退订吗?

支持。

在VPN网关列表页面，选择需要退订的网关，单击“更多”选项中的“退订”按钮。退订包年/包月VPN网关将同时删除该网关下创建的所有连接，且操作不可逆。

退订后包年/包月网关会退还剩余的预支付费用。

2.4.8 VPN 资源在什么情况下会被冻结，如何解除被冻结的 VPN 资源?

- 包年/包月的VPN资源在到期未续费时会进入宽限期，宽限期内您可正常访问及使用该资源。宽限期结束后，若您仍未续订，该资源将进入保留期，即被冻结状

 版权所有 © 华为技术有限公司

态。被冻结的资源不可用，也不能修改、删除。超过保留期仍未续费，冻结资源将被释放，被释放资源不可恢复。为确保资源持续可用，请在资源到期前及时续费。

- 按需的VPN资源在欠费时将资源置于欠费状态并进入宽限期，宽限期内您可正常访问及使用该资源。宽限期结束后，若您仍未缴清欠款，该资源将进入保留期，即被冻结状态。被冻结的资源不可用，也不能修改、删除。超过保留期仍未充值缴清欠费金额，冻结资源将被释放，被释放资源不可恢复。为确保资源持续可用，请在资源到期前完成充值，并确保所欠金额已结清。
- 冻结的VPN资源在续费或充值后会变为可用状态。需要注意的是，VPN连接的状态可能出现“未连接”，请发起数据流（如子网间主机互ping）触发VPN连接至“正常”状态。

2.4.9 VPN 资源如何扣费，如何使用优惠券?

VPN网关计费模式分为按需和包年/包月。计费模式以实际region购买界面为准。

- 按需为后付费，根据资源使用情况从账号余额中扣除费用。
- 包年/包月为预付费，创建资源时一次性扣除。

如果您已获得云优惠券，请在优惠券有效期内完成充值，充值后可按抵用资源使用费。

包年/包月资源在创建包年资源时会产生优惠费用，实际支付时费用可扣减。

合同用户需要在控制台页面选择“申请线上合同请款后支付”。

2.5 Console 与页面使用

2.5.1 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。

 版权所有 © 华为技术有限公司

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。

2.5.2 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。

2.5.3 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。

2.5.4 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。

2.5.5 创建 VPN 是需要创建 VPN 网关还是 VPN 连接，已经创建的 VPN 哪些信息可以修改，哪些信息不可以修改?

创建VPN的前置条件:

需要先创建VPC及VPC子网，且VPC的子网不能与用户侧数据中心IDC子网冲突。

创建VPN包括创建VPN网关和VPN连接两个步骤。

- 创建VPN网关：分配了网关IP和带宽信息，在创建时需要选择区域、名称、计费模式、关联VPC、计费方式、带宽大小。其中区域、计费模式，关联VPC、计费方式创建完成后不可修改。

 版权所有 © 华为技术有限公司

- 创建VPN连接：VPN连接需要指定连接的名称、关联已创建的VPN网关、指定本端子网、预共享密钥、远端网关、远端子网和协商策略信息。其中连接名称、本端子网、预共享密钥、远端网关、远端子网和协商策略在创建完成后可以修改。

2.5.6 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?

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。

2.5.7 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。

2.5.8 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远端子网路由，无需手动配置。

2.5.9 华为云是否支持 API?

VPN属于比较复杂的业务配置，目前暂不支持通过API创建，查询，修改资源，请用户通过管理控制台来操作。

2.5.10 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。

2.5.11 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。

 版权所有 © 华为技术有限公司

2.5.12 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。

2.5.13 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）。

2.5.14 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”。

2.5.15 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）；

如果页面长时间停留在删除或创建中，请**提交工单**解决。

2.5.16 无带宽信息的网关无法创建新的连接如何解决?

经典版VPN网关无带宽显示，说明该网关为老版VPN的产品，云已不支持创建该版本的产品。

- 老版VPN在使用过程中带宽无法保障，一个网关只能创建一条连接，用户可以删除网关后重建（影响业务）；
- 用户也可以**提交工单**处理，工作人员会在后台将该网关变更为新版VPN网关（不影响业务）。

  默认情况下变更至新版VPN网关的带宽规格为10M，用户后期可根据实际需要调整带宽大小； 变更后转为包年/包月的网关支持到期后续费带宽降配。

 版权所有 © 华为技术有限公司

2.5.17 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。

2.5.18 VPN 网关最大支持多大带宽?

VPN网关规格最大支持100Mbit/s。

2.5.19 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。

 版权所有 © 华为技术有限公司

  - 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

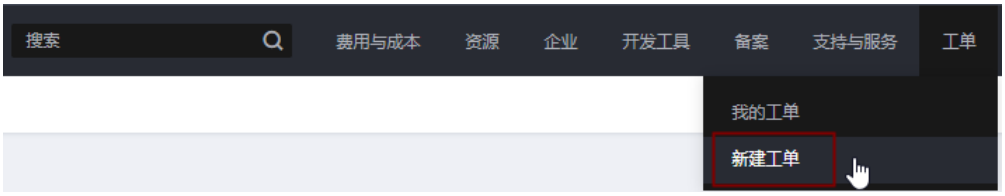
- 简化了安全联盟的协商过程，提高了协商效率。
- 修复了多处公认的密码学方面的安全漏洞，提高了安全性能。
- 加入对EAP（Extensible Authentication Protocol）身份认证方式的支持，提高了认证方式的灵活性和可扩展性。
- EAP是一种支持多种认证方法的认证协议，可扩展性是其最大的优点，即如果想加入新的认证方式，可以像组件一样加入，而不用变动原来的认证体系。当前EAP认证已经广泛应用于拨号接入网络中。
- IKEv2使用基于ESP设计的加密载荷，v2加密载荷将加密和数据完整性保护关联起来，即加密和完整性校验放在相同的载荷中。AES-GCM同时具备保密性、完整性和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

2.5.20 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”。

 版权所有 © 华为技术有限公司

图 2-13 新建工单



3. 搜索并选择“VPN”。

图 2-14 选择工单产品分类

4. 选择问题类型。

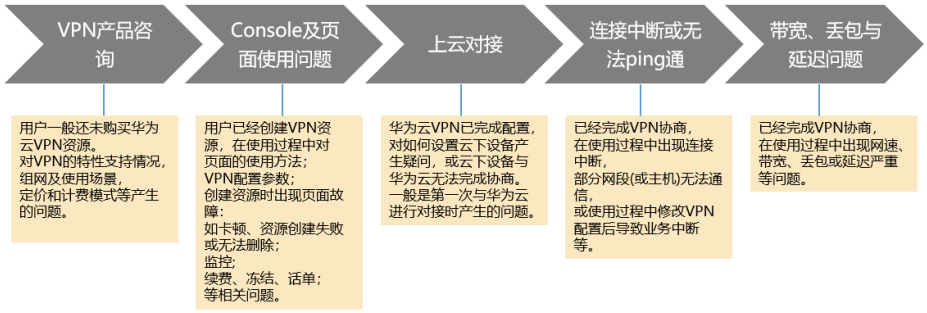
图 2-15 选择问题类型

 版权所有 © 华为技术有限公司

说明

用户在**提交工单**时请选择相应的问题类型，有助于加速问题处理。

图 2-16 问题类型与分类依据



2.5.21 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。

2.5.22 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”。

详细请参见**支持的监控指标**。

2.5.23 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。

2.6 VPN 协商与对接

版权所有 © 华为技术有限公司

2.6.1 哪些设备可以与云进行 VPN 对接?

VPN支持标准IPsec协议，用户可以通过以下两个方面确认用户侧数据中心的设备能否与云进行对接：

1. 设备是否具备IPsec功能和授权：请查询设备的特性列表获取是否支持IPsec VPN。
2. 关于组网结构，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）也可以。

设备型号多为路由器、防火墙等，对接配置请参见**管理员指南**。

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。
- 与VPN服务做过对接测试厂商包括：
  - 设备厂商：华为（防火墙/AR）、山石（防火墙），CheckPoint（防火墙）。
  - 云服务厂商包括：阿里云，腾讯云，亚马逊（aws），微软（Microsoft Azure）。
  - 软件厂商包括：strongSwan。
- IPsec协议属于IETF标准协议，宣称支持该协议的厂商均可与云进行对接，用户不需要关注具体的设备型号。

  目前绝大多数企业级路由器和防火墙都支持该协议。
- 部分硬件厂商在特性规格列表中是宣称支持IPsec VPN的，但是需要专门购买软件License才能激活相关功能。

  请用户侧数据中心管理员根据设备具体型号与厂商进行确认。

2.6.2 VPN 协商参数有哪些? 默认值是什么?

表 2-5 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）

版权所有 © 华为技术有限公司

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）

版权所有 © 华为技术有限公司

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。

2.6.3 IPsec VPN 是否会自动建立连接?

IPsec VPN在完成两侧配置后，并不会自行建立连接，需要两侧主机间的数据流来触发隧道的建立。如果云上与用户侧数据中心间没有交互数据流，VPN的连接状态会一直处于Down状态。所谓的数据流，可以是真实的业务访问数据，也可以是主机间Ping测数据。

 版权所有 © 华为技术有限公司

触发隧道建立的方式有两种，一种是通过建立连接间的网关设备自动触发协商，另一种是通过云上云下主机间的交互流量触发。

云暂不支持通过云端VPN网关自动触发协商。推荐您在首次建立连接时，分别验证两侧的交互数据流均可触发连接建立。即用户侧数据中心主机ping云上主机可触发连接建立，然后断开连接，确认云上主机Ping用户侧数据中心主机亦可触发连接建立。

说明

Ping包的源地址、目的地址需要处于VPN保护的范围内。

在建立连接之前，两端的网关地址应该是可以Ping通的，但是Ping网关IP并不触发VPN连接的建立。

2.6.4 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。

2.6.5 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。

2.6.6 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。

2.6.7 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

 版权所有 © 华为技术有限公司

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。

2.6.8 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。

2.6.9 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。

2.6.10 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。

 版权所有 © 华为技术有限公司

2.6.11 华为云的 VPN 对接 AWS 后，为何不可以从 AWS 向华为云的 VPN 发起协商?

华为云的VPN建立连接完成后，AWS为Response模式，并不主动发起协商，当从AWS的EC2向华为云ECS发起数据流时，也不触发该VPN建立SA。

按照AWS的知识文档，默认从客户侧（即对接AWS的云）发起被动协商，也支持修改为主动协商。

2.6.12 多个子网对接 Ali 云，为何协商不成功?

多子网对接Ali云，按照Ali云的配置要求，只能选择IKEv2进行对接；

在华为云上需要按照两端子网的乘积来配置对应数量的连接，如云本端有2个子网，Ali云有3个子网，在华为云上需要配置6条连接，每条连接仅包含一条感兴趣流。

2.6.13 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。

2.6.14 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。

2.6.15 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。

 版权所有 © 华为技术有限公司

- 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。

2.6.16 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2-6所示。

表 2-6 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。

2.6.17 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2-7所示。

表 2-7 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

 版权所有 © 华为技术有限公司

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

2.7 连接故障或无法 PING 通

2.7.1 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。

2.7.2 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；
- 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；
- 两端子网进行长Ping操作（脚本内容如下）。

```
#!/bin/sh
host=$1
if [ -z $host ]; then
```

 版权所有 © 华为技术有限公司

```
    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。

2.7.3 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。详细请参见**2.12.1 如何防止VPN连接出现中断情况?** 。
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**提交工单**向客服寻求帮助。

 版权所有 © 华为技术有限公司

2.7.4 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)。

2.7.5 IPsec VPN 是否会自动建立连接?

IPsec VPN在完成两侧配置后，并不会自行建立连接，需要两侧主机间的数据流来触发隧道的建立。如果云上与用户侧数据中心间没有交互数据流，VPN的连接状态会一直处于Down状态。所谓的数据流，可以是真实的业务访问数据，也可以是主机间Ping测数据。

触发隧道建立的方式有两种，一种是通过建立连接间的网关设备自动触发协商，另一种是通过云上云下主机间的交互流量触发。

暂不支持通过云端VPN网关自动触发协商。推荐您在首次建立连接时，分别验证两侧的交互数据流均可触发连接建立。即用户侧数据中心主机ping云上主机可触发连接建立，然后断开连接，确认云上主机Ping用户侧数据中心主机亦可触发连接建立。

说明

Ping包的源地址、目的地址需要处于VPN保护的范围内。

在建立连接之前，两端的网关地址应该是可以Ping通的，但是Ping网关IP并不触发VPN连接的建立。

2.7.6 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。

2.7.7 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。

2.7.8 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。

 版权所有 © 华为技术有限公司

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。

2.7.9 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，如华为的NQA，或cisco的ip sla。

2.7.10 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。

2.7.11 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。

2.7.12 如何解决 VPN 连接无法建立连接问题?

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

   假设您的数据中心的子网为192.168.3.0/24和192.168.4.0/24，VPC下的子网为192.168.1.0/24和192.168.2.0/24，则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。

2.7.13 VPN 建立后您的数据中心或局域网无法访问弹性云服务器?

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

 版权所有 © 华为技术有限公司

2.7.14 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。

2.7.15 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。

2.7.16 什么是对等体存活检测?

DPD（Dead Peer Detection，对等体存活检测）用于检测对端是否存活。本端主动向对端发送DPD请求报文，检测对端PEER是否存活。

- 如果本端在DPD报文的重传时间间隔内未收到对端回应的DPD报文，则重传DPD请求报文，当到达最大重传次数之后仍然没有收到对端的DPD回应报文，则认为对端已经离线，本端将删除该IKE SA和对应的IPsec SA，同时发送报文通知对端。
- DPD报文是一个双向交换的消息，该消息包含通知载荷（notify）和Hash载荷（hash）。

  发起者发送的通知载荷携带R-U-THERE消息，相当于一个Hello报文，响应者发送的通知载荷携带R-U-THERE-ACK消息，相当于一个ACK报文。

  不同设备缺省发出的DPD报文的载荷顺序可能不同，而两端IKE对等体的DPD报文中的载荷顺序需要一致，否则对等体存活检测功能将无法生效。

  IKE对等体间进行IPsec通信时，除DPD报文中的载荷顺序需要匹配外，DPD检测中其它配置参数两端不需要匹配。当IKE对等体间有正常的IPsec流量时，不会发送DPD消息，只有当一段时间内收不到对端发来的IPsec报文时，才发送DPD消息。

 版权所有 © 华为技术有限公司

DPD 核心配置

DPD的核心配置包含检测模式、检测时间、报文格式等。以华为设备为例，配置DPD的方法有全局配置和IKE对等体两种方式。IPsec通信时，优先使用IKE对等体的DPD配置参数，如果对等体未配置DPD，则采用全局DPD配置参数。

- **检测模式：**分为按需和周期性检测。华为设备缺省配置中无全局检测配置，是否开启对等体检测要看对等体的DPD配置是否使能。

  按需型：当本端需要向对端发送IPsec报文时，如果当前距离最后一次收到对端的IPsec报文的时长已超过DPD空闲时间，则触发DPD检测，本端主动向对端发送DPD请求报文。

  周期型：如果当前距离最后一次收到对端的IPsec报文的时长已超过DPD空闲时间，则本端主动向对端发送DPD请求报文。
- **DPD配置参数：**包含DPD空闲时间、DPD报文重传间隔和重传次数，华为设备缺省情况下全局DPD空闲时间、DPD报文重传间隔和重传次数分别为30秒、15秒和3次。
- **报文格式：**有seq-hash-notify和seq-notify-hash两种。华为设备缺省情况下，DPD报文中的载荷顺序为seq-hash-notify。

⚠ 注意

当IPsec两端未配置DPD报文时，如果隧道内无流量，会等待SA的生命周期到期。到期前会发起硬协商，如果协商未成功则拆除本端SA，同时通知对端。SA的恢复需要再次进行数据流触发协商才能建立。

如果因为网络原因一端拆除SA，另一端没有拆除SA，会导致业务流量不通，需要等待SA生命周期老化或手工清除SA。

DPD 配置说明

检测模式：按需。

检测时间：空闲时间30s，重传间隔15s，重传次数3次。

报文格式为：seq-hash-notify。

2.8 公网地址

2.8.1 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。

版权所有 © 华为技术有限公司

2.8.2 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。

2.8.3 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。

2.8.4 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。

2.8.5 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。

2.9 路由设置

2.9.1 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。

2.9.2 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。

 版权所有 © 华为技术有限公司

2.9.3 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。

2.10 VPN 子网设置

2.10.1 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）。

2.10.2 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。

2.10.3 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。

2.10.4 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。

2.10.5 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。

版权所有 © 华为技术有限公司

- 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。

2.10.6 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。

2.10.7 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225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。

2.11 VPN 感兴趣流

2.11.1 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。

2.11.2 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。

 版权所有 © 华为技术有限公司

2.12 VPN 连接保活

2.12.1 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 &
```

 版权所有 © 华为技术有限公司

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。

2.13 监控类

2.13.1 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”。

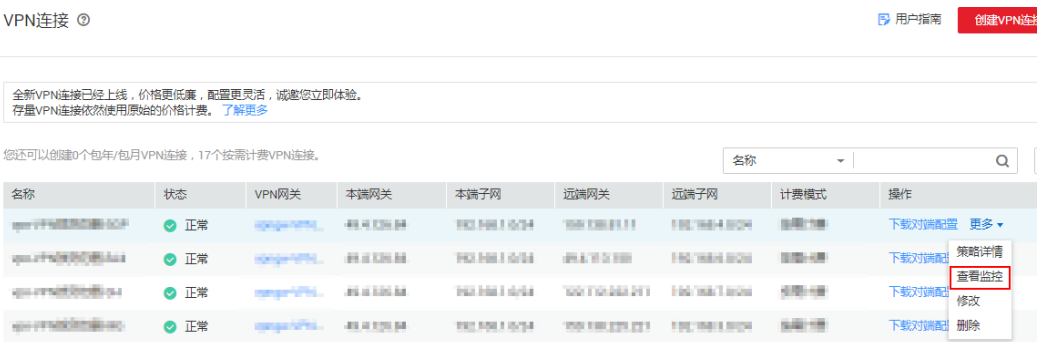
详细请参见**支持的监控指标**。

2.13.2 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。

图 2-17 查看 VPN 连接监控



 版权所有 © 华为技术有限公司

2.13.3 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。

详细请参见**查看监控指标**。

2.13.4 当 VPN 监控结果异常时，可以发送提醒信息吗?

可以。

用户可以通过配置“消息通知服务”和 “云监控服务”实现VPN监控结果异常提醒。

配置消息通知服务

1. 登录管理控制台。
   选择“管理与监管 > 消息通知服务”
2. 选择“主题 > 创建主题”，创建一个主题，如VPN-huaweicloud。
3. 选择“订阅 > 添加订阅”。
   调用主题，协议选择邮件，终端填写接收消息的Email地址。

   说明

   添加订阅后系统会给您的Email发送一封确认邮件，请在您的Email中进行确认。

配置云监控服务

1. 登录管理控制台。
   选择“管理与监管 > 云监控服务”
2. 创建VPN网关带宽使用率告警规则。
   填写名称，资源类型选择弹性公网IP和带宽，维度选择带宽，监控范围指定资源为特定的VPN网关，选择类型自定义创建，告警策略选择带宽使用率，可选连续5个周期大于90%进行告警。发送通知的对象选择消息通知服务的主题，其它配置项默认。
3. 创建VPN连接状态告警规则。
   创建过程与带宽类同。资源类型选择虚拟专用网络，监控范围指定资源为特定的VPN连接，选择类型自定义创建，告警策略选择连接状态小于1时进行告警。发送通知的对象选择消息通知服务的主题，其它配置项默认。
4. 创建用户侧数据中心IDC链路监控告警规则。
   创建站点监控，类型选择Ping，站点地址选择用户侧数据中心网关IP，其它信息默认。创建告警规则，资源类型选择站点监控，监控范围指定创建资源，告警策略选择可探测点数量小于选择的探测点数。发送通知的对象选择消息通知服务的主题，其它配置项默认。

2.14 带宽与网速

2.14.1 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。

 版权所有 © 华为技术有限公司

当用户购买的VPN网关的带宽为200Mbit/s时，测试情况如下。

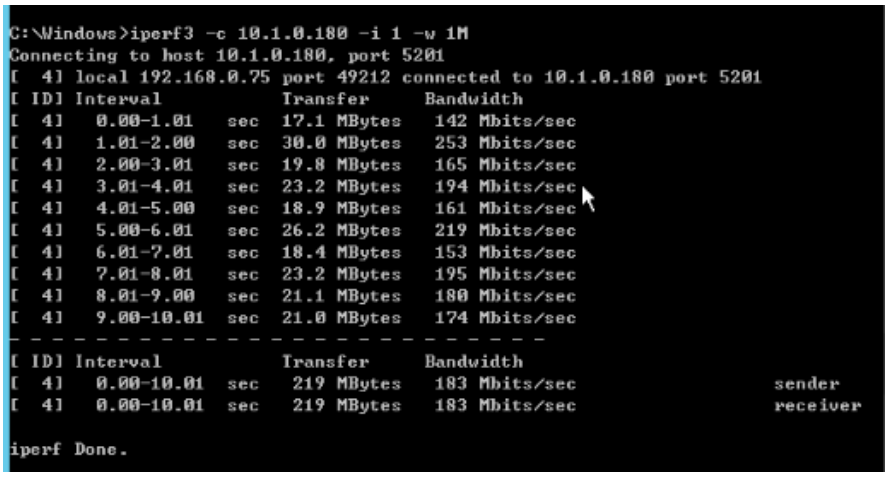
1. 互为对端的ECS都使用Windows系统，测试速率可达180Mbit/s，使用iperf3和filezilla（是一款支持ftp的文件传输工具）测试均满足带宽要求。

   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。

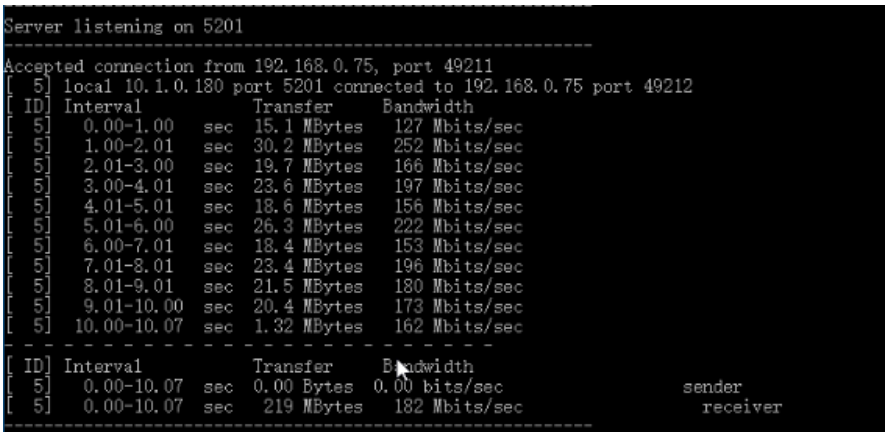
   使用iperf3客户端测试结果截图如图2-18所示。

   图 2-18 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2-19所示。

   图 2-19 200M 带宽服务端 iperf3 测试结果

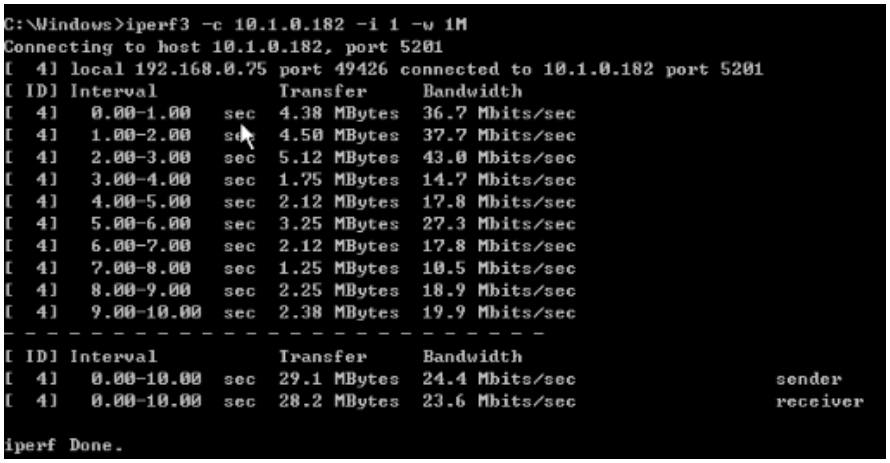
2. 互为对端的ECS都使用Centos7系统，测试速率可达180M，使用iperf3测试满足带宽要求。
3. 服务器端ECS使用Centos7系统，客户端使用Windows系统，测试速率只有20M左右，使用iperf3和filezilla测试均不能满足带宽要求。

   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2-20所示。

 版权所有 © 华为技术有限公司

图 2-20 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。具体ECS的规格可参见**ECS规格**。

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。

2.14.2 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。

2.14.3 如何修改 VPN 的带宽大小?

1. 在VPN网关列表页目标VPN网关所在行，选择“更多 > 修改带宽”。
2. 在修改带宽页面选择带宽大小。
3. 单击“提交”，完成修改。

说明

- 按需的VPN可自由修改带宽大小。
- 包年/包月的VPN只可进行带宽扩容，不可降低带宽大小。

2.14.4 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。

 版权所有 © 华为技术有限公司

说明

VPN的带宽最大为300(Mbit/s)。

2.14.5 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。

2.14.6 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。

2.14.7 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，详细请参见**VPN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)。

  说明

  华北-北京四区域VPN最大带宽为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。

2.14.8 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。

2.15 配额类

 版权所有 © 华为技术有限公司

2.15.1 虚拟专用网络的配额是什么?

什么是配额?

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少台弹性云服务器、多少块云硬盘。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

怎样查看我的配额?

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

如何申请扩大配额?

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

2.15.2 创建 VPN 网关和连接的缺省配额是多少?

- VPN：每个用户缺省可创建50个VPN网关和100个远端网关。请在购买VPN网关前确认您可用的配额，如果选购信息超出可用配额可**提交工单**申请扩容。
- 经典版VPN：每个用户缺省可创建2个VPN网关和12个VPN连接。请在购买VPN网关前确认您可用的配额，如果选购信息超出可用配额可**提交工单**申请扩容。

2.15.3 如何修改当前客户的 VPN 网关和连接的配额?

1. 进入管理控制台，在界面右上方选择“工单管理 > 新建工单 ”
2. 选择问题所属产品：选择“业务类 > 配额类”。
3. 选择问题类型：单击“配额申请”。
4. 新建工单：单击“新建工单”。
   填写区域、问题描述等信息，单击“提交”。

2.15.4 一个用户下支持多少个 IPsec VPN?

默认情况下，每个用户可以创建2个VPN网关，12条VPN连接。

如果用户实际使用网关或连接超出缺省配额，可**提交工单**申请。

 版权所有 © 华为技术有限公司

配额中VPN网关数量不得大于VPC数量，连接数配额超过200请向VPN产品经理申请。

2.16 账号权限

2.16.1 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。

2.16.2 创建 VPN 时系统提示权限不足，如何处理?

请确认您的账号是否为子账号，如果未开通VPC操作权限，请使用主账号在统一身份认证服务（IAM）中对您的账号进行授权。确保具有“VPC Administrator”、“Tenant Guest”、“VPN Administrator”这三个【系统角色】权限。

详细操作请参见**创建用户组并授权**和**用户组添加用户**。

2.16.3 如何确定我的账号是因为权限不足而无法创建 VPN 的?

- 主账号创建的VPN网关和连接，子账号不可见。
- 创建VPN网关或连接时提示系统繁忙。

账号创建VPN连接所需权限详见**2.16.2 创建VPN时系统提示权限不足，如何处理?**

版权所有 © 华为技术有限公司

3 终端入云 VPN

3.1 如何测试终端入云 VPN 网关的带宽

如果您需要测试终端入云VPN网关的带宽，推荐您使用iPerf3工具进行测试。若使用FTP、SCP等命令的话，传输文件的速率由于受到磁盘读写速度的影响无法反映真实的带宽速率。

前提条件

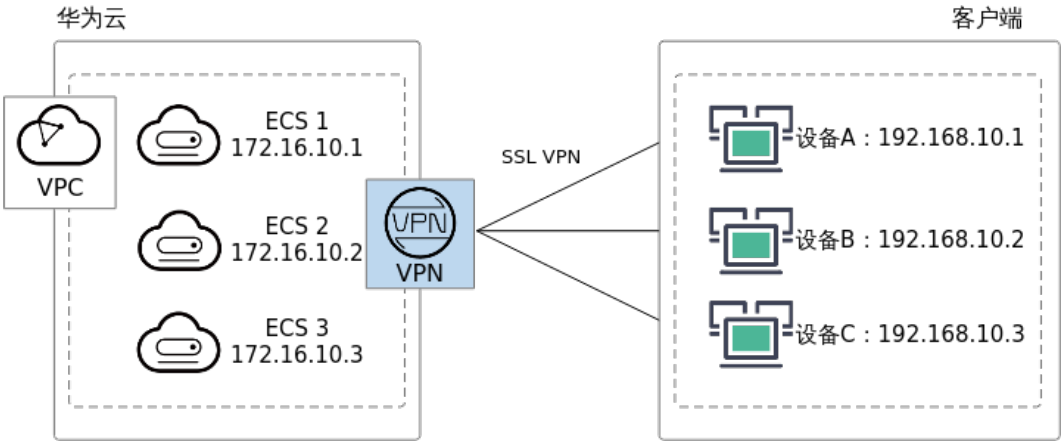
- 已完成VPN网关和服务端的相关配置，客户端可以正常连接VPN网关。
  本示例中，VPN网关规格为专业型1（最大转发带宽300Mbps）。
- 已部署3个ECS实例，位于VPN网关所在VPC网络中，用于模拟云上的资源节点。
  本示例中，每个ECS实例规格均为c6.large.2（vCPUs：2，内存：4GB，系统镜像：CentOS 8.0-64bit）。
- 已准备3个云下设备，模拟接入客户端。
  本示例中，设备A、设备B为Linux服务器（4U8G，运行ubuntu-20.04.6-live-server-amd64操作系统），设备C为PC（i7处理器，运行Windows 10操作系统）。
- 云下设备、ECS接口和网络的带宽能力满足要求（上、下行带宽不低于100Mbps）。
- 云下设备到VPN网关的网络质量较好。

组网场景

本文介绍如何使用iPerf3工具测试VPN网关带宽，组网场景如**图 组网场景**所示。

 版权所有 © 华为技术有限公司

图 3-1 组网场景



安装 iPerf3

此处以在本次测试使用的云下设备上安装iPerf3为例。

在Linux上安装iPerf3

1. 打开命令行窗口。
2. 执行以下命令，安装iPerf3。
   yum install -y iperf3
3. 执行以下命令，查看是否安装成功。
   iperf3 -v
   若系统回显iPerf版本信息，表示安装成功。

在Windows上安装iPerf3

在iPerf3官方网站**下载iPerf3**，根据操作系统版本下载对应软件。

使用 iPerf3 测试 VPN 网关的带宽

iPerf3概述

iPerf3的主要参数说明如**表3-1**所示。

表 3-1 iPerf3 主要参数说明

主要参数	参数说明
-s	服务端专用参数，表示iPerf3以服务端模式运行。
-c	客户端专用参数，表示iPerf3以客户端模式运行。
-p	指定服务端侦听端口，即客户端需要连接的服务端的端口（服务端和客户端的配置需要保持一致）。
-i	发送数据的时间间隔，单位：秒。

版权所有 © 华为技术有限公司

主要参数	参数说明
-l	设置读写缓冲区的长度。建议该值设为1300，模拟业务数据payload为1300字节。
-P	表示线程个数，不指定则默认单线程。

云下设备作为服务端

1. 在云下设备上执行以下命令，以服务端模式启动iPerf3进程，并指定不同的侦听端口。示例如下：
   - 设备A（Linux）

     iperf3 -s -p 20001
   - 设备B（Linux）

     iperf3 -s -p 20002
   - 设备C（Windows）

     iperf3.exe -s -p 20003
2. 分别在3个ECS实例上，执行以下命令，以客户端模式启动iPerf3进程，并指定云下设备对应的服务端侦听端口。

   iperf3 -c *server-ip* **-p** *server-port* **-l 1300 -P 10**

   示例如下：

```
iperf3 -c 192.168.10.1 -p 20001 -l 1300 -P 10
iperf3 -c 192.168.10.2 -p 20002 -l 1300 -P 10
iperf3 -c 192.168.10.3 -p 20003 -l 1300 -P 10
```

云下设备作为客户端

1. 分别在3个ECS实例上，执行以下命令，以服务端模式启动iPerf3进程并指定不同的侦听端口。

   iperf3 -s -p *server-port*

   示例如下：

```
iperf3 -s -p 20001
iperf3 -s -p 20002
iperf3 -s -p 20003
```

2. 分别在云下设备上，执行以下命令，以客户端模式启动iPerf3进程，并指定ECS实例对应的侦听端口。示例如下：
   - 设备A

     iperf3 -c 172.16.10.1 -p 20001 -l 1300 -P 10
   - 设备B

     iperf3 -c 172.16.10.2 -p 20002 -l 1300 -P 10
   - 设备C

     iperf3.exe -c 172.16.10.3 -p 20003 -l 1300 -P 10

测试结果

iPerf3进程执行完毕后，会显示如下的结果。

```
Connecting to host 172.16.10.1, port 20001
[  4] local 192.168.10.1 port 20001 connected to 172.16.10.1 port 20001
```

 版权所有 © 华为技术有限公司

```
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.00   sec  8.62 MBytes  72.1 Mbits/sec
[  4]   1.00-2.01   sec  9.88 MBytes  82.2 Mbits/sec
[  4]   2.01-3.01   sec  9.88 MBytes  82.9 Mbits/sec
[  4]   3.01-4.00   sec  9.50 MBytes  80.4 Mbits/sec
[  4]   4.00-5.01   sec  9.88 MBytes  82.1 Mbits/sec
[  4]   5.01-6.01   sec  9.62 MBytes  81.2 Mbits/sec
[  4]   6.01-7.00   sec  9.12 MBytes  77.0 Mbits/sec
[  4]   7.00-8.01   sec  10.0 MBytes  83.2 Mbits/sec
[  4]   8.01-9.01   sec  9.50 MBytes  79.9 Mbits/sec
[  4]   9.01-10.01  sec  8.62 MBytes  72.4 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.01  sec  94.6 MBytes  79.3 Mbits/sec                  sender
[  4]   0.00-10.01  sec  94.6 MBytes  79.3 Mbits/sec                  receiver
```

根据上述iperf3测试的结果，从192.168.10.1到172.16.10.1的连接中，传输速率大约是79.3 Mbits/sec。整个测试持续了10秒钟，期间发送了94.6MB的数据。

3.2 终端入云 VPN 网关是否支持域名访问

支持域名访问。用户可以通过域名直接访问云上业务。

3.3 云证书与管理服务 CCM 中上传证书失败

3.3.1 上传证书时报错，提示“证书链长度必须大于 1”

故障现象

上传证书到云证书与管理服务CCM时报错，提示“证书链长度必须大于1”。

可能原因

证书文件中没有上传该证书的上级CA证书。

约束条件

云证书与管理服务CCM中上传证书之前，需要确保已经生成服务端证书、CA证书和服务端私钥。如何生成证书，具体请参考**通过Easy-RSA自签发证书（服务端和客户端共用CA证书）**。

处理步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“终端入云VPN网关”进入“终端入云VPN网关”页面，单击目标VPN网关操作列的“查看服务端”。

 版权所有 © 华为技术有限公司

步骤6 在“服务端”界面，将服务端证书配置为“已有证书”，在下拉选项中单击“上传证书”进入“云证书与管理服务”页面。

步骤7 在“SSL证书管理”页面，选择“上传证书 > 上传证书”。

步骤8 以记事本或Notepad++打开服务端证书。

步骤9 将证书内容复制到”证书文件”栏目文本框中。

证书文件格式如下：

```
-----BEGIN CERTIFICATE-----
此处添加服务端证书
-----END CERTIFICATE-----
```

步骤10 以记事本或Notepad++打开颁发服务端证书的CA证书。

步骤11 继续将证书内容复制到”证书文件”栏目文本框中。

证书文件格式如下：

```
-----BEGIN CERTIFICATE-----
此处添加服务端证书
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
此处添加CA证书
-----END CERTIFICATE-----
```

步骤12 以记事本或Notepad++打开服务端证书的私钥。

步骤13 将私钥内容复制到”证书私钥”栏目文本框中。

证书私钥格式如下：

```
-----BEGIN PRIVATE KEY-----
此处添加服务端私钥
-----END PRIVATE KEY-----
```

步骤14 点击“确认”按钮，上传成功。

----结束

3.3.2 上传证书时报错，提示“上传证书域名格式错误”

故障现象

上传证书到云证书与管理服务时报错，提示“上传证书域名格式错误”。

可能原因

证书的域名格式不符合规范，正确的格式应该是“xxx.com”、“xxx.cn”等。

处理步骤

步骤1 重新生成符合规范的证书。如何生成证书，具体请参考**通过Easy-RSA自签发证书（服务端和客户端共用CA证书）**。

步骤2 登录管理控制台。

步骤3 进入云证书与管理服务，上传证书。

 版权所有 © 华为技术有限公司

如何上传证书，具体请参考**通过云证书与管理服务CCM托管服务端证书**。

----结束

3.4 客户端连接失败，无报错信息，一直处在连接中

故障现象

客户端连接时无报错信息，一直处在连接中。

可能原因

- 客户端设备无法正常访问Internet网络。
- 客户端版本不符合要求。

处理步骤

1. 请确认客户端可以ping通云上网关eip地址。
2. 如果是Windows操作系统，建议关闭防火墙后重试。
3. 建议OpenVPN客户端版本为2.5及以上。

如果上述操作仍然无法解决客户端登录问题，请**提交工单**联系华为工程师。

版权所有 © 华为技术有限公司