虚拟专用网络

用户指南

文档版本	01
发布日期	2025-11-13

华为技术有限公司

商标声明


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

注意

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

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

安全声明

漏洞处理流程

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

1 站点入云 VPN 企业版

1.1 企业版 VPN 网关管理

1.1.1 创建 VPN 网关

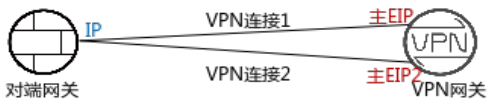
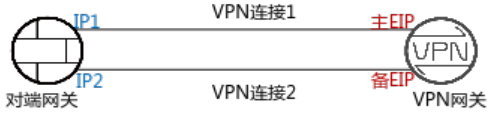
场景描述

如果您需要将VPC中的弹性云服务器和您的数据中心或私有网络连通，创建VPN连接之前，需要创建VPN网关。

背景信息

根据对端网关IP地址个数不同，推荐的组网如表1-1所示。

表 1-1 组网关系

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

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

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

约束与限制

- 非国密型网关不支持变更为国密型网关。
- 关联企业路由器场景下，需要关注企业路由器的路由表条数规格限制。
- 创建VPN网关支持直接创建共享型带宽的EIP，2个EIP要选择同一个共享带宽。
- 非固定IP接入的特性仅在部分区域上线，且仅支持“计费模式”采用“包年/包月”的公网网关场景。
- 本地可用区的特性仅在部分区域上线，以管理控制台实际上线区域为准。
- 专业型3网关不支持IPv6和非固定IP接入，且不支持边缘可用区。

前提条件

- 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
- 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。
- 如果通过企业路由器ER关联VPN网关，请确认企业路由器ER已经创建完成。如何创建企业路由器ER，请参见企业路由器ER相关资料。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“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 在“站点入云VPN网关”界面，单击“创建站点入云VPN网关”。

步骤6 根据界面提示配置参数，单击“立即购买”。

VPN网关参数请参见**表1-2**。

表 1-2 VPN 网关参数说明

参数	说明	取值样例
计费模式	• 包年/包月：预付费方式，在创建VPN网关阶段按月或按年收取费用，默认包含10个VPN连接组的费用。 • 按需计费：后付费方式，VPN网关和VPN连接组按使用时长收取费用，计费周期为1小时。	包年/包月 按需计费

参数	说明	取值样例
区域	选择靠近您所在地域的区域可以降低网络时延，从而提高访问速度。 不同区域的资源之间网络不互通。	亚太-新加坡
可用区	可用区是指在同一地域内，电力和网络互相独立的物理区域。在同一VPC网络内可用区与可用区之间内网互通，可用区之间能做到物理隔离。建议您根据VPC内资源所在的可用区选择网关的可用区类型。 ● 通用可用区 ● 本地可用区	*请根据实际设置*
名称	VPN网关的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	vpngw-001
网络类型	● 公网：VPN网关通过公网建立VPN连接。 ● 私网：VPN网关通过私网建立VPN连接。	公网
协议类型	支持“IPv4”和“IPv6”两种类型。	IPv4
关联模式	● 虚拟私有云 通过VPC向对端网关或本端子网内服务器发送通信消息。当可用区选择本地可用区时，“关联模式”仅支持“虚拟私有云”。 ● 企业路由器 通过ER向对端网关或ER下所有VPC所在子网发送通信消息。 **说明** 该场景下需要关注企业路由器的路由表条数规格限制。如果对端网关和VPN网关发送的路由条数超过企业路由器的规格，则企业路由器将无法学习到超出部分的路由信息，最终导致VPN网关和对端网关之间的流量不通。	虚拟私有云
虚拟私有云	仅“关联模式”采用“虚拟私有云”时需要配置。 选择虚拟私有云VPC信息。	vpc-001(192.168.0.0/16)
企业路由器	仅“关联模式”采用“企业路由器”时需要配置。 选择企业路由器ER信息。	er-001
接入虚拟私有云	“关联模式”采用“企业路由器”时需要配置。 当VPN网关的南北向需要连接不同的虚拟私有云时，设置北向的虚拟私有云为该接入虚拟私有云。	vpc-001(192.168.0.0/16)
接入子网	“关联模式”采用“企业路由器”时需要配置。 VPN网关连接公网的子网。	subnet-001(192.168.0.0/24)

参数	说明	取值样例
网关接入IP	“关联模式”采用“企业路由器”、“网络类型”为“私网”时需要配置。 ● 自动分配IP地址（默认） 使用接入子网对VPN网关分配网关IP。 自动分配的私网网关IP，可以在“VPN网关”页面进行查看。 ● 手动指定IP地址 指定接入子网中的IP地址配置VPN网关IP。	自动分配IP地址
互联子网	仅“关联模式”采用“虚拟私有云”时需要配置。 用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.66.0/24
本端子网	仅“关联模式”采用“虚拟私有云”时需要配置。 配置VPC与对端网关对应数据中心互通的子网。 ● 选择子网 选择本VPC子网信息。 ● 输入网段 可以输入本VPC下的子网信息；也可以输入与本VPC建立了对等网络的VPC子网信息。	192.168.1.0/24,192.168.2.0/24
BGP ASN	VPN网关会根据输入值创建相应的ASN，VPN网关和对端网关的BGP ASN需要不同。 BGP AS号取值范围为1-4294967295。	64512
HA模式	● 双活 – 关联模式选择“虚拟私有云”时，对端子网和哪个EIP先创建VPN连接1，则VPN网关到该对端子网的出云流量优先走VPN连接1。VPN连接1故障失效后，出云流量会自动切换到该对端子网的另一条VPN连接2；故障失效的VPN连接1恢复后，出云流量会仍然通过VPN连接2，不会切回到VPN连接1。 – 关联模式选择“企业路由器”时，VPN网关到该对端子网的出云流量由该对端子网对应的所有VPN连接负载分担。 ● 主备 VPN网关到该对端子网的出云流量优先走该对端子网和主EIP建立的VPN连接1。VPN连接1失效后，出云流量自动切换到该对端子网和备EIP建立的VPN连接2；故障失效的VPN连接1恢复后，出云流量会自动切回到VPN连接1。	双活
规格	支持基础型、专业型1、专业型2、专业型3、国密型五种类型。 仅“网络类型”为“公网”且“计费模式”采用“包年/包月”时，专业型1、专业型2支持非固定IP接入。	专业型1

参数	说明	取值样例
VPN连接组数	仅“计费模式”采用“包年/包月”时需要配置。 VPN网关默认提供10个免费的VPN连接组。 • 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。	10
是否使用共享带宽	• “计费模式”采用“包年/包月”时，默认开启使用共享带宽。 • “计费模式”采用“按需计费”时，默认不开启使用共享带宽。	不开启
弹性公网IP类型	选择VPN网关绑定EIP的类型。 弹性公网IP类型的详细介绍请参见**什么是弹性公网IP**。	*请根据实际设置*
本地线路	仅“弹性公网IP类型”采用“本地线路”时需要配置。	*请根据实际设置*
带宽名称	仅“网络类型”采用“公网”时需要配置。 EIP对应带宽对象的名称。 • 带宽Mbit/s：5 • 当“是否适用共享带宽”采用开启使用共享带宽时，可选择共享带宽的名称。 • 单个共享带宽最多可以添加弹性公网IP的个数：20。如需申请更多配额，请参考**如何申请扩大配额？**。	Vpngw-bandwidth2
主EIP	仅“网络类型”采用“公网”时需要配置。 用于VPN网关和对端网关进行网络连接。 • 现在创建：购买新EIP，新购买EIP的计费模式跟VPN网关的计费模式保持一致。 **说明** 使用共享带宽时仅支持现在创建EIP。 • 使用已有：使用已有EIP，支持与其他网络服务的EIP共享带宽。	现在创建

参数	说明	取值样例
公网带宽	仅“计费模式”采用“按需计费”、“网络类型”采用“公网”时需要配置。 按需计费支持两种计费方式： • 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。 • 按流量计费：指定带宽上限，按实际使用的出云流量计费，与使用时间无关。	按流量计费
带宽大小	仅“网络类型”采用“公网”时需要配置。 EIP对应带宽大小，单位：Mbit/s。 • 所有使用该EIP创建的VPN连接均会分摊占用该EIP的带宽大小，所有VPN连接的带宽总和不能超过该EIP的带宽大小。 当网络流量超过EIP的带宽大小时，有可能造成网络拥塞导致VPN连接中断，请提前做好带宽规划。 • 支持在云监控中配置告警规则对带宽进行监控。 • 支持用户在允许的带宽范围内自定义带宽大小。 • 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。	10 Mbit/s
主EIP2	仅“网络类型”采用“公网”、“HA模式”选择“双活”时需要配置。 一个VPN网关需要绑定一组弹性公网IP（即主EIP、主EIP2），每个公网IP可以独立规划带宽和付费方式，也可以与其他网络服务的EIP共享带宽。 **说明** 使用共享带宽时仅支持现在创建EIP，且创建完成后不支持修改。	现在创建
备EIP	仅“网络类型”采用“公网”、“HA模式”选择“主备”时需要配置。 一个VPN网关需要绑定一组弹性公网IP（即主/备EIP），每个公网IP可以独立规划带宽和付费方式，也可以与其他网络服务的EIP共享带宽。 **说明** VPN网关“计费模式”为“按需计费”场景下，若备EIP为按流量计费，强烈建议用户在云监控中配置告警规则对备EIP进行监控，避免因VPN连接故障、主链路切换至备链路导致的流量费用超支问题。 如何在云监控中对EIP配置告警规则，请参见**创建告警规则**。	现在创建

参数	说明	取值样例
企业项目	创建VPN时，可以将VPN加入已启用的企业项目。 企业项目管理提供了一种按企业项目管理云资源的方式，帮助您实现以企业项目为基本单元的资源及人员的统一管理，默认项目为default。 关于创建和管理企业项目的详情，请参见**《企业管理用户指南》**。	default
高级配置	仅“网络类型”为“私网”、“关联模式”采用“虚拟私有云”时需要配置。 ● 选择：适用于同租户场景，选择本租户下接入虚拟私有云、接入子网、网关接入IP。 ● 输入：适用于跨租户场景，填写接入项目、接入账号、接入虚拟私有云、接入子网和网关接入IP。	选择
接入项目	仅“高级配置”中配置方式选择“输入”方式时配置。 输入接入项目ID，如何获取对应项目ID请参见**如何获取企业项目ID**。	*请根据实际设置*
接入账号	仅“高级配置”中配置方式选择“输入”方式时配置。 输入接入账号ID，如何获取对应账号ID请参见**查看或修改IAM用户信息**。	*请根据实际设置*
接入虚拟私有云	● “关联模式”采用“企业路由器”时需要配置。 ● “关联模式”采用“虚拟私有云”、“网络类型”为“私网”时需要配置。 当VPN网关的南北向需要连接不同的虚拟私有云时，设置北向的虚拟私有云为该接入虚拟私有云。VPN网关关联的虚拟私有云为南向业务虚拟私有云。	选择“与网关关联的虚拟私有云一致”
接入子网	● “关联模式”采用“企业路由器”时需要配置。 ● “关联模式”采用“虚拟私有云”、“网络类型”为“私网”时需要配置。 缺省情况下，VPN网关从关联的虚拟私有云的互联子网接入。当VPN网关需要从指定子网接入时设置。	选择“与互联子网一致”

参数	说明	取值样例
网关接入IP	“关联模式”采用“虚拟私有云”、“网络类型”为“私网”时需要配置。 ● 自动分配IP地址（默认） 使用接入子网对VPN网关分配网关IP。 自动分配的私网网关IP，可以在“VPN网关”页面进行查看。 ● 手动指定IP地址 指定接入子网中的IP地址配置VPN网关IP。 “高级配置”中配置方式选择“选择”方式时，单击右侧“查看已使用IP地址”可查看已使用IP地址，支持刷新和模糊匹配搜索功能。 VPN网关“HA模式”选择“主备”时，依次配置为主IP、备IP；“HA模式”选择双活时，依次配置为主IP、主IP2。	自动分配IP地址
高级设置/标签	VPN服务的资源标签，包括键和值，最大可以创建20对标签。 标签设置时，可以选择预定义标签，也可以自定义创建。 预定义标签可以通过单击“查看预定义标签”进行查看。	-
购买时长	仅“计费模式”采用“包年/包月”时需要配置。 在账户余额充足场景下，如果勾选“自动续费”功能，系统会在当前服务购买时长到期后自动进行续费。 ● 按月购买场景，自动续费周期为一个月。 ● 按年购买场景，自动续费周期为一年。	6

步骤7 确认订单详情，单击“去支付”。

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

上传VPN网关证书的相关操作请参见**上传VPN网关证书**。

----结束

1.1.2 查看已创建的 VPN 网关

场景描述

用户创建VPN网关后，可以查看已创建的VPN网关。

操作步骤

1. 登录管理控制台。

2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，查看VPN网关列表信息。
6. 单击VPN网关的名称，查看VPN网关详情。
   - 公网类型网关：可查看基本信息、弹性公网IP、标签和路由信息；若VPN网关规格为“专业型1-非固定IP”或“专业型2-非固定IP”，还可查看策略模板。
   - 私网类型网关：可查看基本信息、高级配置和路由信息。
   - 国密型网关：可查看基本信息、证书信息和路由信息。

说明

- 在VPN网关列表中，选择目标VPN网关所在行，单击网关IP列的 ，查看该VPN网关带宽和流量的监控信息。
- 在站点入云VPN网关列表页面，可以看到“导出”和设置按钮。
  - 选择左上方的导出，在下拉框中选择需要导出的数据。
  - 单击右上方的 ，根据需要设置自定义显示列。

1.1.3 修改已创建的 VPN 网关

场景描述

您可以对VPN网关基本信息进行修改，包括名称、本端子网。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，单击目标VPN网关操作列的“修改基本信息”。

   若仅需修改VPN网关的名称，您也可以直接单击VPN网关名称右侧的按钮进行修改。
6. 根据界面提示，修改VPN网关的名称、本端子网。
7. 单击“确定”。

VPN网关参数修改请参见**VPN网关参数修改说明**。

表 1-3 VPN 网关参数修改说明

参数	说明	是否支持修改
名称	VPN网关的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	支持
EIP	可以通过先解绑EIP，然后绑定EIP的方式对EIP进行修改。 如果EIP已经创建了VPN连接，则无法解绑。 **说明** • 仅支持修改带宽大小。 • EIP的名称和弹性公网IP类型需要到EIP界面修改。	支持
本端子网	VPC与对端网关对应数据中心互通的子网。	支持
计费模式	包括包年/包月和按需计费。	支持
VPN连接组数	仅“计费模式”为“包年/包月”时需要设置。	支持
区域	选择靠近您所在地域的区域可以降低网络时延，从而提高访问速度。 不同区域的资源之间网络不互通。	不支持
规格	支持基础型、专业型1、专业型2、专业型3、国密型五种类型。	部分支持，以管理控制台界面为准
关联模式	包括虚拟私有云和企业路由器。	不支持
企业路由器	仅“关联模式”为“企业路由器”时需要设置。	不支持
虚拟私有云	选择需要和用户数据中心通信的VPC。	不支持
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	不支持
BGP ASN	BGP自治系统号码。	不支持

参数	说明	是否支持修改
可用区	可用区是指在同一地域内，电力和网络互相独立的物理区域。在同一VPC网络内可用区与可用区之间内网互通，可用区之间能做到物理隔离。 ● 当存在两个及以上可用区时，必须选择两个可用区。部署在两个可用区的VPN网关具备更高的可用性。建议您根据VPC内资源所在的可用区选择网关的可用区。 ● 当仅存在一个可用区时，可选择此可用区创建VPN网关。	不支持

1.1.4 修改 VPN 网关规格

场景描述

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

- 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。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，单击目标VPN网关操作列的“更多 > 修改规格”，或者单击操作列的“修改规格”。
6. 根据界面提示，完成修改网关规格操作。

1.1.5 修改 VPN 网关策略模板

场景描述

若VPN网关规格为“专业型1-非固定IP”或“专业型2-非固定IP”，您可以在VPN网关页面修改策略模板。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，单击目标VPN网关操作列的“查看/修改策略模板”，在“策略模板”页签下单击“修改策略模板”进行修改。

   说明

   修改策略模板后，以非固定IP接入的对端网关需要更新对应配置重新接入，否则会导致连接中断。

表 1-4 策略模板参数说明

参数		说明	是否支持修改
IKE策略	版本	IKE密钥交换协议版本，支持v2。	×
	认证算法	认证哈希算法，支持的算法： ● SHA2-256 ● SHA2-384 ● SHA2-512 默认配置为：SHA2-256。	√
	加密算法	加密算法，支持的算法： ● AES-128-GCM-16 ● AES-256-GCM-16 ● 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） 默认配置为：AES-128	√

参数		说明	是否支持修改
	DH算法	支持的算法： ● 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。	√
	生命周期（秒）	安全联盟（Security Association，SA）的生存时间。 在超过生存时间后，安全联盟将被重新协商。 ● 单位：秒。 ● 取值范围：60~604800 默认配置为：86400。	√
	本端标识	IPsec连接协商时，VPN网关的鉴权标识。在对端网关配置的VPN网关标识需要和此处配置的本端标识保持一致，否则协商失败。 默认配置为：VPN网关的EIP。	×
IPsec策略	认证算法	认证哈希算法，支持的算法： ● SHA2-256 ● SHA2-384 ● SHA2-512 默认配置为：SHA2-256。	√
	加密算法	加密算法，支持的算法： ● AES-128-GCM-16 ● AES-256-GCM-16 ● 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） 默认配置为：AES-128。	√

参数		说明	是否支持修改
	PFS	PFS（Perfect Forward Secrecy）即完美前向安全功能，配置IPsec隧道协商时使用。 PFS组支持的算法： ● 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 ● Disable 默认配置为：DH group 15。	√
	传输协议	IPsec传输和封装用户数据时使用的安全协议。 目前支持的协议：ESP。	×
	生命周期（秒）	安全联盟（Security Association，SA）的生存时间。 在超过生存时间后，安全联盟将被重新协商。 ● 单位：秒。 ● 取值范围：30~604800 默认配置：3600。	√

6. 单击“确定”。

1.1.6 绑定弹性公网 IP

场景描述

用户根据需要为已创建的VPN网关绑定EIP。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，单击目标VPN网关操作列的“绑定EIP”。

- 如果VPN网关是双活模式，VPN网关支持绑定主EIP/主EIP2。
- 如果VPN网关是主备模式，VPN网关支持绑定主/备EIP。

6. 根据界面提示，选择需要绑定的EIP，单击“确定”。

1.1.7 解绑弹性公网 IP

场景描述

用户创建VPN网关后，可以解绑已关联的弹性公网IP。

约束与限制

已创建VPN连接的EIP不支持解绑操作。

操作步骤

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

说明

- 未绑定VPN网关的弹性公网IP会继续计费，如果不再使用建议释放。
- 当共享带宽冻结时，EIP的行为以EIP资源为准。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？**。

1.1.8 退订包年/包月 VPN 网关

场景描述

当无需使用包年/包月购买的VPN网关时，可退订VPN网关。

约束与限制

- 仅VPN网关状态正常时可执行退订操作。
- 如果VPN网关绑定了按需计费的弹性公网IP，VPN网关退订时将自动解绑弹性公网IP，解绑后弹性公网IP继续保留，若不再使用可在网关退订后释放。

操作步骤

1. 登录管理控制台。

2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，选择需要退订的VPN网关操作列的“更多 > 退订”。
6. 根据界面提示，完成退订操作。

1.1.9 续费包年/包月 VPN 网关

场景描述

当包年/包月购买的VPN网关临近过期时，可以对VPN网关进行续费操作。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，选择需要续费的VPN网关操作列的“更多 > 续费”，或单击操作列的“续费”。
6. 根据界面提示，完成续费操作。

1.1.10 删除 VPN 网关

场景描述

当无需使用VPN网关时，可以删除VPN网关。

约束与限制

- 在VPN网关状态处于“创建中”、“更新中”、“删除中”三种状态时，不能进行VPN网关删除操作。
- 如果VPN网关绑定的EIP计费模式为包年/包月，删除VPN网关时会同步解绑EIP。解绑后弹性公网IP继续保留，若不再使用可在网关删除后释放。
- 如果VPN网关绑定的EIP计费模式为按需，删除VPN网关时会同步释放EIP。

  如果需要保留按需EIP，则您需要先将该EIP解绑，然后再删除VPN网关。如何解绑EIP，请参见**1.1.7 解绑弹性公网IP**。
- 如果VPN网关绑定了加入共享带宽的EIP，删除VPN网关时会同步释放EIP，保留共享带宽。

操作步骤

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

3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，选择需要删除的VPN网关操作列的“更多 > 删除”，或者单击操作列的“删除”。
6. 在“删除VPN网关”的弹窗页，单击“一键输入”。
7. 单击“确定”。

说明

当共享带宽冻结时，EIP的行为以EIP资料为准。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？**。

1.1.11 上传 VPN 网关证书

场景描述

国密型VPN网关，需要上传证书，用于和对端网关建立VPN连接；首次使用国密型网关，用户需要在云监控页面配置云监控告警，详细步骤请参见**创建事件监控的告警通知**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，选择需要上传证书的国密型VPN网关操作列的“更多 > 查看/上传证书”。
6. 单击“上传证书”，根据界面提示填写相关信息。

   VPN网关证书参数请参见**表1-5**。

表 1-5 VPN 网关证书参数说明

参数	说明	取值样例
证书名称	用户自定义。	certificate-001
签名证书	签名证书用于对数据进行签名认证，以保证数据的有效性和不可否认性。 以文本编辑器（如Notepad++）打开签名证书PEM格式的文件，将证书内容复制到此处。 签名证书需要同时上传签发此签名证书的CA证书。	-----BEGIN CERTIFICATE----- *签名证书* -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- *CA证书* -----END CERTIFICATE-----

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

1.1.12 更换 VPN 网关证书

场景描述

国密型VPN网关证书到期或失效后，需要更换VPN网关证书。

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

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在“站点入云VPN网关”界面，选择需要上传证书的国密型VPN网关操作列的“更多 > 查看/上传证书”。
6. 单击“更换”，根据界面提示填写相关信息。

   VPN网关证书参数请参见**表1-6**。

表 1-6 VPN 网关证书参数说明

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

7. 勾选“我已知晓上述内容，确认更换证书”，单击“确定”。

1.1.13 按标签搜索 VPN 网关

场景描述

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

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

前提条件

已为VPN资源添加标签，详细操作请参见**为云资源添加标签**。

操作步骤

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

1.1.14 升级网关实例

升级概述

用户可以在VPN网关列表页，根据是否有升级按钮来判断您的VPN网关是否为最新版本，并根据实际需要判断是否需要升级。

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

当升级状态处于“请确认是否完成升级”时，用户可以根据实际需要进行回退操作。

约束与限制

如果VPN网关、EIP或共享带宽的计费模式为包周期，只有当距离到期时间超过1天时，才能进行网关实例的升级和回退操作。

升级影响

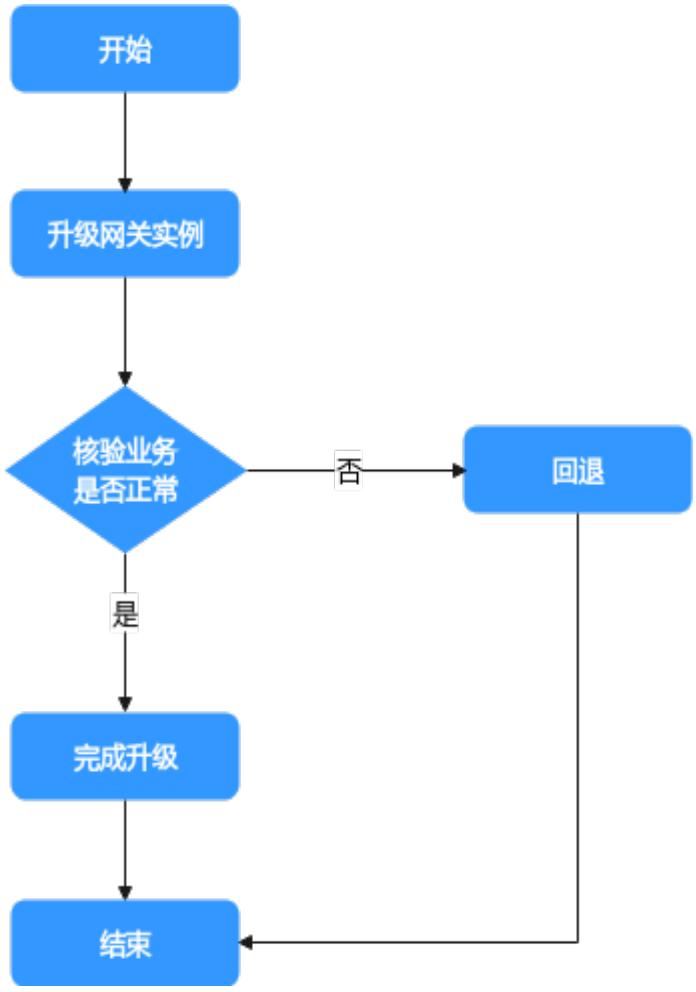
- 升级中VPN连接会出现中断，中断时间大约为10分钟。
- 升级中VPN网关以及其VPN连接均无法操作。

回退机制

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

操作步骤

图 1-1 升级流程示意图



步骤1 升级网关实例。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在“站点入云VPN网关”界面，选择目标VPN网关，单击操作列的“升级网关实例”。
5. 在弹窗中了解升级影响和回退机制，勾选“我已知晓以上升级须知”后，单击确定。
6. 查看升级状态。实例升级过程中，可以在VPN网关列表页的状态列单击查看任务，查看升级进展。
   - 如果实例升级成功，网关状态会刷新为请确认是否完成升级，进入步骤2。
   - 如果实例升级失败，会自动回滚。可以在VPN网关列表页的右上方，查看失败信息。

步骤2 验证业务是否正常。

1. 业务正常，单击操作列的“完成升级”。

须知

单击“完成升级”后，升级任务无法回退，请谨慎选择。

2. 业务异常，单击操作列的“回退”，请**提交工单**联系华为工程师。

----结束

1.2 企业版对端网关管理

1.2.1 创建对端网关

场景描述

如果您需要将VPC中的弹性云服务器和您的数据中心或私有网络连通，创建VPN连接之前，需要创建对端网关。

约束与限制

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

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-对端网关”。
5. 在“对端网关”界面，单击“创建对端网关”。
6. 根据界面提示配置参数，单击“立即创建”。

   对端网关参数请参见**表1-7**。

表 1-7 对端网关参数说明

参数	说明	取值样例
名称	对端网关的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	cgw-001

参数	说明	取值样例
标识	• IP Address：使用对端网关的网关IP作为IP Address。 不支持输入以0开头的网关IP，如0.xx.xx.xx。 • FQDN：全地址域名，支持自定义设置。长度范围是1~128个字符，只能由大小写字母、数字和特殊符号组成，不支持以下特殊字符：&、<、>、[、]、\、空格、？，区分大小写。 如果对端网关无固定IP，请选择FQDN类型标识。 请确认本地数据中心或私有网络中的防火墙规则已经放通UDP端口4500。	• IP Address，1.2.3.4 • FQDN，cgw-fqdn
BGP ASN	请输入用户数据中心或私有网络的ASN。 对端网关的BGP ASN与VPN网关的BGP ASN不能相同。	65000
CA证书（可选）	使用国密型网关时，需要上传对端网关的CA证书，用于和VPN网关建立VPN连接。 • 上传证书：手动输入，以“-----BEGIN CERTIFICATE-----”作为开头，以“-----END CERTIFICATE-----”作为结尾。 • 使用已上传证书：查看并勾选已上传证书，请注意证书到期时间。	-----BEGIN CERTIFICATE----- *CA证书* -----END CERTIFICATE-----
高级配置/标签	VPN服务的资源标签，包括键和值，最大可以创建20对标签。 标签设置时，可以选择预定义标签，也可以自定义创建。 预定义标签可以通过单击“查看预定义标签”进行查看。	-

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

相关操作

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

1.2.2 查看已创建的对端网关

场景描述

用户创建对端网关后，可以查看已创建的对端网关。

操作步骤

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

1.2.3 修改已创建的对端网关

场景描述

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

添加或更换CA证书相关操作请参见**1.2.5 上传对端网关证书**和**1.2.6 更换对端网关证书**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-对端网关”。
5. 在“对端网关”界面，选择目标对端网关所在行，单击 。
6. 修改对端网关名称，单击“确定”。
   对端网关参数修改请参见**对端网关参数修改说明**。

表 1-8 对端网关参数修改说明

参数	说明	是否支持修改
名称	VPN连接的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	支持
高级配置/标签	VPN服务的资源标签，包括键和值。	支持
BGP ASN	BGP自治系统号码。	不支持

参数	说明	是否支持修改
标识	对端网关和VPN网关通信的IP地址，该网关IP地址值必须是静态地址。	不支持

1.2.4 删除对端网关

场景描述

用户根据实际需要删除已创建的对端网关。

约束与限制

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

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-对端网关”。
5. 在“对端网关”界面，选择目标对端网关所在行，单击操作列的“删除”。
6. 确定要删除的对端网关信息，单击“确定”。

1.2.5 上传对端网关证书

场景描述

国密型对端网关，需要上传对端网关的CA证书，用于和VPN网关建立VPN连接。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-对端网关”。
5. 在“对端网关”界面，单击目标对端网关名称进入详情页面。
6. 在“CA证书”区域，单击“添加”。
7. 根据界面提示填写相关信息，单击“确定”。
   对端网关CA证书参数请参见**表1-9**。

表 1-9 对端网关 CA 证书参数说明

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

1.2.6 更换对端网关证书

场景描述

国密型网关CA证书到期或失效后，需要更换CA证书。

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

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-对端网关”。
5. 在“对端网关”界面，单击目标对端网关名称进入详情页面。
6. 在“CA证书”区域，单击“更换”。
7. 根据界面提示填写相关信息。
   对端网关CA证书参数请参见**表1-10**。

表 1-10 对端网关 CA 证书参数说明

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

8. 勾选“我已知晓上述内容，确认更换CA证书”，单击“确定”。

1.2.7 按标签搜索对端网关

场景描述

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

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

前提条件

已为VPN资源添加标签，详细操作请参见**为云资源添加标签**。

操作步骤

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

1.3 企业版 VPN 连接管理

1.3.1 创建 VPN 连接

场景描述

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

约束与限制

- 使用静态路由模式创建VPN连接时，使能NQA前请确认对端网关支持ICMP功能，且对端接口地址已在对端网关上正确配置，否则可能导致流量不通。
- 使用策略模式创建VPN连接时，若添加多条策略规则，源、目的网段要避免出现重叠，以免造成数据流误匹配或IPsec隧道震荡。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
5. 在“VPN连接”页面，单击“创建VPN连接”。

   说明

   VPN网关的两个EIP支持和对端网关创建一组VPN连接，VPN双连接可以很大程度提升云上云下连接的可靠性。
6. 根据界面提示配置参数，单击“立即购买”。

   VPN连接参数请参见**表1-11**。

表 1-11 VPN 连接参数说明

参数	说明	取值样例
名称	VPN连接的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	vpn-001
VPN网关	选择待关联的VPN网关名称。 您也可以单击“创建VPN网关”进行新建，相关参数解释请参见**表1-2**。 如果您使用国密型VPN网关，且VPN网关没有绑定相关证书，请先单击右侧“上传证书”完成上传证书操作，否则VPN连接将无法建立。	vpngw-001
连接1网关IP	• 当“网络类型”采用“公网”时，网关IP为VPN网关的主EIP。 • 当“网络类型”采用“私网”时，网关IP为VPN网关的主IP。 VPN网关对接同一对端网关时，不能选择已使用过的地址。	11.xx.xx.11
连接1对端网关	选择连接1对端网关。 您也可以单击“创建对端网关”进行新建，相关参数解释请参见**表1-7**。 如果您使用国密型网关，且对端网关没有绑定CA证书，请先参见**1.2.5 上传对端网关证书**上传CA证书，否则VPN连接将无法建立。 **说明** 如果一个对端网关同时对接多个VPN网关，则VPN网关的BGP ASN和连接模式需要相同。	cgw-001

参数	说明	取值样例
连接2网关IP	• 当“网络类型”采用“公网”、“HA模式”选择“双活”时，网关IP为VPN网关的主EIP2。 • 当“网络类型”采用“私网”、“HA模式”选择“双活”时，网关IP为VPN网关的主IP2。 • 当“网络类型”采用“公网”、“HA模式”选择“主备”时，网关IP为VPN网关的备EIP。 • 当“网络类型”采用“私网”、“HA模式”选择“主备”时，网关IP为VPN网关的备IP。 同一VPN网关和同一对端网关连接使用的网关IP不能相同。	11.xx.xx.12
连接2对端网关	选择连接2对端网关。 您也可以单击“创建对端网关”进行新建，相关参数解释请参见**表1-7**。 如果您使用国密型网关，且对端网关没有绑定CA证书，请先参见**1.2.5 上传对端网关证书**上传CA证书，否则VPN连接将无法建立。 **说明** 如果一个对端网关同时对接多个VPN网关，则VPN网关的BGP ASN和连接模式需要相同。	cgw-001

参数	说明	取值样例
连接模式	IPsec连接的模式，支持路由模式和策略模式。 ● 静态路由模式。 根据路由配置（本端子网与对端子网）确定哪些数据进入IPsec VPN隧道。 **适用场景：对端网关之间要求互通。** ● BGP路由模式。 根据BGP动态路由确定哪些数据进入IPsec VPN隧道。 **适用场景：对端网关之间要求互通、互通子网数量多或变化频繁、与专线互备等组网场景。** ● 策略模式。 根据策略规则（用户侧到VPC之间通信的数据流信息）确定哪些数据进入IPsec VPN隧道，支持以源网段和目的网段定义策略规则。 **适用场景：对端网关之间要求隔离。** ● 策略模板模式。 仅“VPN网关”为非固定IP网关规格、“对端网关”为FQDN类型时，支持策略模板模式。 VPN网关被动响应对端网关的IPsec连接请求，认证对端网关后接受对端网关以源网段和目的网段定义的策略规则。 – VPN不支持对端设备配置策略的源和目的子网时使用地址组配置。 – 策略模板模式只支持ikev2。 **适用场景：对端网关无固定IP地址。** **说明** 当创建双连接时，默认两个连接的连接模式、对端子网、分支互联开关（BGP路由模式）和策略规则（策略模式）一致。	静态路由模式

参数	说明	取值样例
对端子网	指需要通过VPN连接访问云上VPC的用户侧子网。 若存在多个对端子网，请用半角逗号（,）隔开。 **说明** • 对端子网可以和本端子网重叠，但不能重合。 • 对端子网不能被VPN网关关联的VPC内已有子网所包含；不能作为被VPN网关关联的VPC自定义路由表的目的地址。 • 对端子网不能是VPC的预留网段，例如100.64.0.0/10、100.64.0.0/12、214.0.0.0/8。不同region的预留网段不同，实际使用以控制台显示为准。如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。 • 如果互联子网关联了ACL规则，则需要确保ACL规则中已放通所有本端子网到对端子网的TCP协议端口。 • VPN不支持对端设备配置策略的源和目的子网时使用地址组配置。 • 当“关联模式”采用“企业路由器”，“连接模式”采用“BGP路由模式”、“策略模板模式”和“策略模式”时，无需配置对端子网。	172.16.1.0/24,172.16.2.0/24
分支互联	“连接模式”采用“BGP路由模式”，支持分支互联功能。 • 开启 开启状态的对端网关可以学到本端子网的路由，也可以学到其他对端网关的路由。 • 关闭 关闭状态的对端网关只能学到本端子网的路由，不可以学到其他对端网关的路由。 默认关闭。 **说明** 关闭时只发布本端子网路由。	关闭

参数	说明	取值样例
策略规则	仅“连接模式”采用“策略模式”时需要配置。 用于定义本端子网到对端子网之间具体进入VPN连接加密隧道的数据流信息，由源网段与目的网段来定义。系统默认支持配置5条策略规则。 ● 源网段。 源网段必须包含部分本端子网。其中，0.0.0.0/0表示任意地址。一个VPN连接最大支持5个源网段。 ● 目的网段。 目的网段必须完全包含对端子网。一个策略规则最大支持50个目的网段，目的网段之间使用英文逗号（,）进行分隔。	● 源网段1：192.168.1.0/24 ● 目的网段1：172.16.1.0/24,172.16.2.0/24 ● 源网段2：192.168.2.0/24 ● 目的网段2：172.16.1.0/24,172.16.2.0/24
连接1配置	配置连接1网关IP的接口地址分配方式、本端隧道接口地址、对端隧道接口地址、检测机制、预共享密钥、确认密钥、策略配置和高级配置。	请根据实际设置

参数	说明	取值样例
接口地址分配方式	仅“连接模式”采用“静态路由模式”和“BGP路由模式”时需要配置。 **说明** • 接口地址为VPN网关和对端网关通信的tunnel隧道IP地址。 • 如果对端网关的tunnel接口地址固定不可更改，请使用“手动分配”模式，并根据对端网关的tunnel接口地址设置VPN网关的tunnel接口地址。 ● 手动分配 – 仅支持在169.254.x.x/30网段（除169.254.195.x/30）范围内，配置VPN网关本端接口地址的tunnel接口地址；对端网关对端接口地址的tunnel接口地址会根据本端接口地址自动生成。例如：本端接口地址配置为169.254.1.6/30，则对端接口地址自动配置为169.254.1.5/30。 – 当“连接模式”采用“BGP路由模式”的场景下，选择“手动分配”的方式配置隧道接口地址时，对端设备VPN连接的隧道接口地址需要与本端隧道地址配置成镜像地址。 ● 自动分配 – VPN网关默认使用169.254.x.x/30网段对tunnel接口分配地址。 – 自动分配的本端接口地址/对端接口地址，可以在VPN连接页面，单击“修改连接信息”进行查看。 – 当“连接模式”采用“BGP路由模式”的场景下，选择“自动分配”的方式，在创建连接后，可查看分配的本端隧道接口地址和对端隧道接口地址，对端设备VPN连接的隧道接口地址需要与本端隧道地址配置成镜像地址。	自动分配
本端隧道接口地址	仅“接口地址分配方式”采用“手动分配”时需要配置。 配置在VPN网关上的tunnel接口地址。	-

参数	说明	取值样例
对端隧道接口地址	仅“接口地址分配方式”采用“手动分配”时需要配置。 配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。	-
检测机制	仅“连接模式”采用“静态路由模式”时需要配置。 **说明** 功能开启前，请确认对端网关支持ICMP功能，且对端接口地址已在对端网关上正确配置，否则可能导致流量不通。 功能开启后，VPN网关会自动对对端接口地址进行NQA探测。关于NQA的相关介绍，请参见**华为云NQA**。	勾选
预共享密钥	VPN网关和对端网关的预共享密钥需要保持一致。 取值范围： ● 取值长度：8~128个字符。 ● 只能包括以下几种字符，且必须包含三种及以上类型： – 数字。 – 大写字母。 – 小写字母。 – 特殊符号：包括“~”、“!”、“@”、“#”、“$”、“%”、“^”、“(”、“)”、“-”、“_”、“+”、“=”、“{”、“}”、“,”、“.”、“/”、“:”和“;”。 **说明** 国密型VPN连接无此参数。	Test@123
确认密钥	再次输入预共享密钥。 **说明** 国密型VPN连接无此参数。	Test@123
策略配置	● 默认配置。 ● 自定义配置：自定义配置IKE策略和IPsec策略。相关配置说明请参见**表1-12**和**表1-13**。 **说明** 当本端标识和对端标识类型为IP Address时，支持配置指定标识值，且本端ID与对端ID不能相同。	自定义配置

参数	说明	取值样例
策略模板配置	仅“连接模式”采用“策略模板模式”时需要配置。 此处不支持对策略模板进行修改，如需修改，请参见**1.1.5 修改VPN网关策略模板**中关于修改策略模板的描述。	-
标签	• VPN服务的资源标签，包括键和值，最大可以创建20对标签。 • 标签设置时，可以选择预定义标签，也可以自定义创建。 • 预定义标签可以通过单击“查看预定义标签”进行查看。	-
连接2配置	选择是否“与连接1保持一致”。 • 开启 • 关闭	开启

表 1-12 IKE 策略

参数	说明	取值样例
版本	IKE密钥交换协议版本，支持的版本： • v1（v1版本安全性较低，如果用户设备支持v2版本，建议选择v2） 建立国密型VPN连接，IKE密钥交换协议版本只能为“v1”。 • v2。 国密型VPN连接默认配置为：v1。 非国密型VPN连接默认配置为：v2。	v2
协商模式	仅“版本”采用“v1”时需要配置。 • Main。 当使用国密型VPN网关创建VPN连接时，“协商模式”仅支持“Main”。 • Aggressive。	Main

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： ● SHA1（此算法安全性较低，请慎用）。 ● MD5（此算法安全性较低，请慎用）。 ● SHA2-256。 ● SHA2-384。 ● SHA2-512。 ● SM3。 仅国密型VPN连接选择该认证算法，此时IKE密钥交换协议版本只能为“v1”。 国密型VPN连接默认配置为：SM3。 非国密型VPN连接默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法： ● 3DES（此算法安全性较低，请慎用）。 ● AES-128（此算法安全性较低，请慎用）。 ● AES-192（此算法安全性较低，请慎用）。 ● AES-256（此算法安全性较低，请慎用）。 ● AES-128-GCM-16。 ● AES-256-GCM-16。 选择该加密算法时，IKE密钥交换协议版本只能为“v2”。 ● SM4。 仅国密型VPN连接选择该加密算法，此时IKE密钥交换协议版本只能为“v1”。 国密型VPN连接默认配置为：SM4。 非国密型VPN连接默认配置为：AES-128。	AES-128

参数	说明	取值样例
DH算法	支持的算法： ● Group 1（此算法安全性较低，请慎用）。 ● Group 2（此算法安全性较低，请慎用）。 ● Group 5（此算法安全性较低，请慎用）。 ● Group 14（此算法安全性较低，请慎用）。 ● Group 15。 ● Group 16。 ● Group 19。 ● Group 20。 ● Group 21。 默认配置为：Group 15。 **说明** 国密型VPN连接无此参数。	Group 15
生命周期（秒）	安全联盟（Security Association，SA）的生存时间。 在超过生存时间后，安全联盟将被重新协商。 ● 单位：秒。 ● 取值范围：60~604800。 ● 默认配置为：86400。	86400
本端标识	IPsec连接协商时，VPN网关的鉴权标识。对端网关配置的对端标识需与此处配置的本端标识保持一致，否则协商失败。 ● IP Address（默认）。 – 系统自动读取VPN网关的网关IP作为IP Address，无需用户手动配置。 – 支持配置指定标识值，且本端ID与对端ID不能相同。 ● FQDN。 全地址域名，支持自定义设置。长度范围是1~128个字符，只能由大小写字母、数字和特殊符号组成，不支持以下特殊字符：&、<、>、[、]、\、空格、？，区分大小写。 **说明** 国密型VPN连接无此参数。	IP Address

参数	说明	取值样例
对端标识	IPsec连接协商时，对端网关的鉴权标识。VPN网关配置的对端标识需与对端网关的本端标识保持一致，否则协商失败。 ● IP Address（默认）。 – 系统自动读取对端网关的网关IP作为IP Address，无需用户手动配置。 – 支持配置指定标识值，且本端ID与对端ID不能相同。 ● FQDN。 全地址域名，支持自定义设置。长度范围是1~128个字符，只能由大小写字母、数字和特殊符号组成，不支持以下特殊字符：&、<、>、[、]、\、空格、？，区分大小写。 **说明** 国密型VPN连接无此参数。	IP Address

表 1-13 IPsec 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： ● SHA1（此算法安全性较低，请慎用）。 ● MD5（此算法安全性较低，请慎用）。 ● SHA2-256。 ● SHA2-384。 ● SHA2-512。 ● SM3。 仅国密型VPN连接选择该认证算法。 国密型VPN连接默认配置为：SM3。 非国密型VPN连接默认配置为：SHA2-256。	SHA2-256

参数	说明	取值样例
加密算法	加密算法，支持的算法： ● 3DES（此算法安全性较低，请慎用）。 ● AES-128（此算法安全性较低，请慎用）。 ● AES-192（此算法安全性较低，请慎用）。 ● AES-256（此算法安全性较低，请慎用）。 ● AES-128-GCM-16。 ● AES-256-GCM-16。 ● SM4。 仅国密型VPN连接选择该加密算法。 国密型VPN连接默认配置为：SM4。 非国密型VPN连接默认配置为：AES-128。	AES-128

参数	说明	取值样例
PFS	PFS（Perfect Forward Secrecy）即完善的前向安全功能，配置IPsec隧道协商时使用。 PFS组支持的算法： ● Disable（此算法安全性较低，请慎用）。 ● DH group 1（此算法安全性较低，请慎用）。 ● DH group 2（此算法安全性较低，请慎用）。 ● DH group 5（此算法安全性较低，请慎用）。 ● DH group 14（此算法安全性较低，请慎用）。 ● DH group 15。 ● DH group 16。 ● DH group 19。 ● DH group 20。 ● DH group 21。 默认配置为：DH group 15。 **说明** ● 国密型VPN连接无此参数。 ● 国密型VPN网关和国密型对端网关创建VPN连接时，需要保证国密型对端网关关闭PFS功能，否则会导致VPN连接无法建立。	DH group 15
传输协议	IPsec传输和封装用户数据时使用的安全协议。目前支持的协议： ESP。 默认配置为：ESP。	ESP
生命周期（秒）	安全联盟（Security Association，SA）的生存时间。 在超过生存时间后，安全联盟将被重新协商。 ● 单位：秒。 ● 取值范围：30~604800。 ● 默认配置：3600。	3600

说明

IKE策略指定了IPsec隧道在协商阶段的加密和认证算法，IPsec策略指定了IPsec隧道在数据传输阶段所使用的协议、加密以及认证算法。VPC和数据中心的VPN连接在策略配置上需要保持一致，否则会导致VPN协商失败，进而导致VPN连接建立失败。

以下算法安全性较低，请慎用：

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

  出于部分对端设备不支持安全加密算法的考虑，VPN连接的默认加密算法仍为AES-128。在对端设备功能支持的情况下，建议使用更安全的加密算法。
- **DH算法：**Group 1、Group 2、Group 5、Group 14。

7. 确认VPN连接规格，单击“提交”。

1.3.2 创建健康检查

场景描述

VPN连接创建完成后，添加健康检查可以配置VPN网关向对端网关发送监测报文，统计链路往返时延和丢包率，用于检测连接的质量。开启健康检查不会影响隧道连接。云监控服务提供对VPN连接链路往返时延和丢包率的监控指标，详情请参见**支持的监控指标**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
5. 在“VPN连接”界面，单击目标VPN连接名称，在“基本信息 > 健康检查”区域单击“添加”。
6. 在“添加健康检查”界面，单击“确定”。

1.3.3 查看已创建的 VPN 连接

场景描述

用户创建VPN连接后，可以查看已创建的VPN连接。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
5. 在“VPN连接”界面，查看VPN连接列表信息。
6. 单击VPN连接的名称，查看VPN连接基本信息、策略配置和标签。

- 当连接模式为静态路由模式时，基本信息包括VPN连接信息、健康检查信息。
- 当连接模式为BGP路由模式时，基本信息包括VPN连接信息、健康检查信息和BGP邻居信息。
- 当连接模式为策略模式时，基本信息包括VPN连接信息、策略规则信息和健康检查信息。

说明

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

  在监控视图中，“VPN连接状态”显示为“0”，表示VPN连接未连接；“VPN连接状态”显示为“1”，表示VPN连接已连接；“VPN连接状态”显示为“2”，表示VPN连接处于未知状态。

  在监控视图中，“BGP邻居状态”显示为“0”，表示BGP邻居未建立；“BGP邻居状态”显示为“1”，表示BGP邻居已建立；“BGP邻居状态”显示为“2”，表示BGP邻居处于未知状态。
- 在VPN连接列表中，可以查看双连接的标识。名称/ID前的图标表示一组对端网关相同的VPN连接，如果双连接在分页的边界处，只显示这组连接的一半标识或。

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

  当VPN连接状态显示“未连接”时，可以根据该VPN连接的日志详情来判断VPN未连接的原因，如果日志没有异常仍然显示未连接，请**提交工单**联系华为工程师。
- 在VPN连接页面，可以看到“导出”和设置按钮。
  - 选择左上方的“导出”，在下拉框中选择需要导出的数据。
  - 单击右上方的，根据需要设置自定义显示列。

1.3.4 修改已创建的 VPN 连接

场景描述

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

操作步骤

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

- 策略模板模式创建的VPN连接不支持在“VPN连接”界面修改策略配置，请在“VPN网关”界面进行修改，具体操作请参见1.1.5 修改VPN网关策略模板。
- BGP路由模式创建的VPN连接支持在“修改连接信息”界面修改“分支互联”的开关。

7. 单击“确定”。

⚠ 注意

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

不同参数修改后的生效机制不同，如表1-14所示。

表 1-14 生效机制

场景	参数	生效机制	操作方法
-	预共享密钥	• IKE策略为v1时：修改后下个协商周期生效。 • IKE策略为v2时：重建VPN连接后生效。 **说明** 国密型VPN连接无“预共享密钥”参数。	• IKE策略为v1时 在需要修改的VPN连接所在行，选择“更多 > 重置密钥”，修改VPN连接的预共享密钥。 • IKE策略为v2时 1. 删除当前VPN连接。 2. 重新创建VPN连接。
IKE策略（版本为v1）	加密算法 认证算法 DH算法 协商模式 本端标识 对端标识 生命周期	修改后下个协商周期生效。 **说明** • 国密型VPN连接不支持修改以下参数：“加密算法”、“认证算法”、“协商模式”。 • 国密型VPN连接无以下参数：“DH算法”、“本端标识”、“对端标识”。	在需要修改的VPN连接所在行，单击“修改策略配置”。
	版本	修改后立即生效。 **说明** 国密型VPN连接不支持修改“版本”参数。	

场景	参数	生效机制	操作方法
IKE策略（版本为v2）	加密算法	修改后下个协商周期生效。	在需要修改的VPN连接所在行，单击“修改策略配置”。
	认证算法		
	DH算法		
	生命周期		
	版本	修改后立即生效。	
	本端标识	重建VPN连接后生效。	1. 删除当前VPN连接。 2. 重新创建VPN连接。
	对端标识		
IPsec策略	加密算法	修改后下个协商周期生效。 **说明** • 国密型VPN连接不支持修改以下参数：加密算法、认证算法。 • 国密型VPN连接不包含以下参数：PFS。	在需要修改的VPN连接所在行，单击“修改策略配置”。
	认证算法		
	PFS		
	生命周期		
	传输协议	暂不支持管理控制台修改。	

VPN连接参数修改请参见**VPN连接参数修改说明**。

表 1-15 VPN 连接参数修改说明

参数	说明	是否支持修改
名称	VPN连接的名称，只能由中文、英文字母、数字、下划线、中划线、点组成。	支持
对端网关	用于与VPC内的VPN互通。	支持
对端子网	用户数据中心中需要和华为云VPC通信的子网。	支持
策略配置	包括IKE策略和IPsec策略。	支持
策略规则	包括源网段和目的网段。	支持

参数	说明	是否支持修改
预共享密钥	VPN网关和对端网关的预共享密钥需要保持一致。	支持
计费模式	• 包年/包月：预付费方式，按月或按年收取费用，默认包含10个VPN连接组的费用。 • 按需计费：后付费方式，VPN网关和VPN连接组按使用时长收取费用，计费周期为1小时。	只支持按需转包年/包月
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。	支持
对端隧道接口地址	配置在对端网关上的tunnel接口地址，该接口地址需要和对端网关实际配置的tunnel接口地址保持一致。	支持
分支互联	“连接模式”采用“BGP路由模式”，支持分支互联功能。	支持
弹性公网IP	仅“网络类型”采用“公网”时需要配置。	不支持
私网IP	仅“网络类型”采用“私网”时需要配置。	不支持
VPN网关	已创建的VPN网关。	不支持
标识	对端网关和VPN网关通信的IP地址，该网关IP地址值必须是静态地址。 请确认数据中心或私有网络中的防火墙规则已经放通UDP端口4500。	不支持
接口地址分配方式	本端接口和对端接口地址的分配方式。包括手动分配和自动分配。	不支持
检测机制	用于多链路场景下路由可靠性检测。 **说明** 功能开启前，请确认对端网关支持ICMP功能，且对端接口地址已在对端网关上正确配置，否则会导致VPN流量不通。	不支持

1.3.5 删除 VPN 连接

场景描述

当无需使用VPN网络、需要释放网络资源时，可删除VPN连接。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
5. 在“VPN连接”界面所需删除的VPN连接所在行的操作列，选择“更多 > 删除”。
6. 在“删除VPN连接”的弹窗页，单击“一键输入”。
7. 单击“确定”。

1.3.6 重置 VPN 连接

场景描述

当用户在使用过程中遇到问题时，可以尝试重置VPN连接以解决该问题。

约束与限制

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

注意

重置操作会导致该VPN连接中断，请谨慎操作。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
5. 在目标VPN连接所在行的操作列，选择“更多 > 重置”，单击确定。
6. 查看VPN连接状态。
   在VPN连接页面的状态列，该连接的状态会显示为“重置中”或“未连接”。

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

1.3.7 查看 VPN 连接日志

场景描述

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

约束与限制

VPN连接的连接日志支持查看最近的200条日志信息。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
5. 在“VPN连接”界面，找到目标VPN连接，单击“查看日志”，查看相关日志信息。

   在查看日志的弹窗中，可以导出时间和信息的日志数据。

1.3.8 按标签搜索 VPN 连接

场景描述

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

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

前提条件

已为VPN资源添加标签，详细操作请参见**为云资源添加标签**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

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

1.4 企业版 VPN 费用管理

1.4.1 按需 VPN 网关转包年/包月

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在目标按需VPN网关所在行，选择“更多 > 转包年/包月”。
   - 支持VPN网关和EIP同时转包年/包月；也支持仅VPN网关转包年/包月，EIP继续维持按需计费。

     如果EIP需要和VPN网关一起转包年/包月，则要求VPN网关已绑定的EIP计费模式为按需计费，且使用按带宽计费。
   - VPN网关转包年/包月后费用计算公式

     转包年/包月前，您已经使用了X个VPN连接组，那么转包年/包月后，实际收取的费用为VPN网关费用+（X-10）个VPN连接组费用。
6. 在“转包年/包月”弹窗界面，单击“确定”。
7. 在“按需转包年/包月”界面，确认需要操作的VPN网关信息，选择购买时长。
8. 单击“去支付”，进入支付界面。
9. 在支付界面，确认订单信息，选择优惠和付款方式。
10. 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。

1.4.2 包年/包月 EIP 带宽升配/降配

操作步骤

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

3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 单击VPN网关名称。
6. 在“弹性公网IP”区域，单击“带宽大小”后的“修改”按钮。
7. 在“修改带宽”界面，选择目标带宽大小，单击“下一步”。
8. 单击“去支付”，完成包年/包月按带宽进行带宽升配或降配。
   - 带宽改大在补齐差价后立即生效。
   - 带宽改小只能在续费周期内生效。

1.4.3 包年/包月 VPN 连接组数升配/降配

约束与限制

- 仅非基础型企业版VPN网关支持连接组数升配/降配。
- 不支持修改为比当前已创建的连接组数小。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 在VPN网关所在行，选择“更多 > 修改VPN连接组数”。
6. 在“修改VPN连接组数”界面，选择目标VPN连接组数，单击“下一步”。
7. 如果是升配操作，单击“去支付”；如果是降配操作，单击“确定”。
   - 增加VPN连接组数后，新连接组数将在原来已有的时间周期内立即生效，您需补交新老配置的差价。
   - 减少VPN连接组数后，新连接组数将在原来已有的时间周期内立即生效，系统将会为您退还新老配置的差价。

2 站点入云 VPN 经典版

2.1 经典版 VPN 网关管理

2.1.1 创建 VPN 网关

操作场景

您需要将VPC中的弹性云服务器和您的数据中心或私有网络连通，需要先创建VPN网关。按需计费购买VPN网关时，可以同时购买一条与其关联的VPN连接。

前置条件

- 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
- 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > 经典版 > VPN网关”。
   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。
5. 在“VPN网关”界面，单击“创建VPN网关”。
6. 根据界面提示配置参数，并单击“立即购买”。VPN网关参数请参见**表 VPN网关参数说明**

表 2-1 VPN 网关参数说明

参数	说明	取值样例
计费模式	VPN网关支持按需计费和包年/包月两种计费模式。计费模式以实际region购买界面为准。 按需计费：购买VPN网关时，可以同时购买一条与其相关联的VPN连接。 包年/包月：在创建VPN网关时一次性收费，包含网关带宽费用和固定连接条目的费用，创建条目数内的VPN连接不再额外收取费用。	按需计费
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	亚太-新加坡
名称	VPN网关名称。	vpngw-001
虚拟私有云	VPN接入的VPC名称。	vpc-001
类型	VPN类型。默认为选择“IPsec”。	IPsec
计费方式	按需计费支持两种计费方式：按带宽计费/按流量计费。 计费方式为包年/包月时只支持按宽带计费。 计费方式以实际region购买界面为准。 • 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。 • 按流量计费：指定带宽上限，按实际使用的上行流量计费，与使用时间无关。	按流量计费
带宽大小	本地VPN网关的带宽大小（单位Mbit/s），为所有基于该网关创建的VPN连接共享的带宽，VPN连接带宽总和不超过VPN网关的带宽。 在VPN使用过程中，当网络流量超过VPN带宽时有可能造成网络拥塞导致VPN连接中断，请用户提前做好带宽规划。 可以在CES监控中配置告警规则对带宽进行监控。	10

说明

当用户创建的VPN网关为按需计费时，默认创建一个VPN连接（深圳Region除外），所以需要同时配置与VPN网关关联的VPN连接参数，详细请参见**表2-2**。

表 2-2 VPN 连接参数说明

参数	说明	取值样例
名称	VPN连接名称	vpn-001
VPN网关	VPN连接挂载的VPN网关名称	vpcgw-001
本端子网	本端子网指需要通过VPN访问用户本地网络的VPC子网。支持以下方式设置本端子网： ● 选择子网，表示用户数据中心或者私有网络与您选择的子网进行互通。 ● 手动输入网段，表示用户数据中心或者私有网络与您配置的网段之间进行互通。 **说明** 多个本端子网不支持子网网段重叠。	192.168.1.0/24， 192.168.2.0/24
远端网关	您的数据中心或私有网络中VPN的公网IP地址，用于与VPC内的VPN互通。	-
远端子网	远端子网指需要通过VPN访问VPC的用户本地子网。远端子网网段不能被本端子网网段覆盖，也不能与本端VPC已有的对等连接网段、专线/云连接的远端子网网段重复。 **说明** 多个远端子网不支持子网网段重叠。	192.168.3.0/24， 192.168.4.0/24
预共享密钥	配置在VPC的VPN和您的数据中心的VPN中，配置需要一致。 取值范围： ● 取值长度：6~128个字符。 ● 只能包括以下几种字符： – 数字 – 大小写字母 – 特殊符号：包括“~”、“`”、“!”、“@”、“#”、“$”、“%”、“^”、“(”、“)”、“-”、“_”、“+”、“=”、“[”、“]”、“{”、“}”、“|”、"\"、","、"."、"/"、“:”和“;”	Test@123
确认密钥	再次输入预共享密钥。	Test@123
高级配置	● 默认配置。 ● 自定义配置：自定义配置IKE策略和IPsec策略。相关配置说明请参见**表 IKE策略**和**表 IPsec策略**。	自定义配置

表 2-3 IKE 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： ● MD5（此算法安全性较低，请慎用） ● SHA1（此算法安全性较低，请慎用） ● SHA2-256 ● SHA2-384 ● SHA2-512 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法： ● AES-128 ● AES-192 ● AES-256 ● 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128
DH算法	Diffie-Hellman密钥交换算法，支持的算法： ● Group 1（此算法安全性较低，请慎用） ● Group 2（此算法安全性较低，请慎用） ● Group 5（此算法安全性较低，请慎用） ● Group 14 ● Group 15 ● Group 16 ● Group 19 ● Group 20 ● Group 21 默认配置为：Group 14。 协商双方的dh算法必须一致，否则会导致协商失败。	Group 14
版本	IKE密钥交换协议版本，支持的版本： ● v1（有安全风险不推荐） ● v2 默认配置为：v2。	v2
生命周期（秒）	安全联盟（SA—Security Association）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：86400。	86400

表 2-4 IPsec 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： ● SHA1（此算法安全性较低，请慎用） ● MD5（此算法安全性较低，请慎用） ● SHA2-256 ● SHA2-384 ● SHA2-512 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法： ● AES-128 ● AES-192 ● AES-256 ● 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128
PFS	PFS（Perfect Forward Secrecy）即完美前向安全功能，用来配置IPsec隧道协商时使用。 PFS组支持的算法： ● DH group 1（此算法安全性较低，请慎用） ● DH group 2（此算法安全性较低，请慎用） ● DH group 5（此算法安全性较低，请慎用） ● DH group 14 ● DH group 15 ● DH group 16 ● DH group 19 ● DH group 20 ● DH group 21 默认配置为：DH group 14。	DH group 14
传输协议	IPsec传输和封装用户数据时使用的安全协议，目前支持的协议： ● ESP ● AH ● AH-ESP 默认配置为：ESP。	ESP

参数	说明	取值样例
生命周期（秒）	安全联盟（SA—Security Association）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：3600。	3600

⚠ 注意

以下算法安全性较低，请慎用：

认证算法：SHA1、MD5。

加密算法：3DES。

DH算法：Group 1、Group 2、Group 5。

7. 确认购买的VPN网关信息，单击“提交”。

   VPN网关创建成功后，系统会分配一个公网出口IP，即VPN网关列表中“网关IP”对应显示的IP地址。该网关IP也是用户侧VPN网络配置对应的远端网关IP。

2.1.2 查看已创建的 VPN 网关

操作场景

用户创建VPN网关后，可以查看已创建的VPN网关。

操作步骤

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

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

2.1.3 修改已创建的 VPN 网关

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

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

- 在目标VPN网关所在行的操作列选择“更多 > 修改规格”。

6. 根据界面参数，修改VPN网关的带宽，或者名称和描述信息。
7. 单击确定。

修改 VPN 网关基本信息

操作场景：

用户根据需要修改VPN网关名称和描述信息。

操作步骤：

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > 经典版-VPN网关”。
   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。
5. 在“VPN网关”界面目标VPN网关所在行，选择“更多 > 修改基本信息”。
6. 根据界面参数，修改VPN网关的名称和描述信息。

   说明

   VPN网关名称只能由中文、英文字母、数字、下划线、中划线、点组成。

7. 单击“确定”。

修改 VPN 网关带宽

操作场景：

当VPN网关带宽不能满足需求时，可修改VPN网关带宽。

操作步骤：

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > 经典版-VPN网关”。
   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。
5. 在“VPN网关”界面目标VPN网关所在行，选择“更多 > 修改带宽”。
6. 根据界面参数，重新选择合适的带宽。
7. 单击“提交”。

2.1.4 退订包年/包月 VPN 网关

操作场景

当无需使用包年包月购买的VPN网关时，可退订VPN网关。

说明

- 创建包年/包月网关时不强制创建VPN连接。
- 如果包年/包月网关下已创建VPN连接，退订包年/包月网关后VPN连接会被同步删除，请谨慎操作。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > 经典版 > VPN网关”。
   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。
5. 在“经典版-VPN网关”界面所需退订的VPN网关所在行，单击“更多 > 退订”。
   如果所在region已同步上线企业版VPN，在“经典版”界面所需退订的VPN网关所在行，单击“更多 > 退订”。
6. 根据界面提示，完成退订操作。

2.1.5 删除按需 VPN 网关

操作场景

当无需使用VPN网关时，可删除VPN网关。

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

说明

创建按需网关时强制创建VPN连接，无法直接手动删除。如果您购买的是按需VPN网关，您可以删除VPN网关下的所有VPN连接，VPN网关将会自动被删除。删除VPN连接请参见**2.2.4 删除VPN连接**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在左侧导航栏选择“虚拟专用网络 > 经典版 > VPN网关”。
   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。
4. 在“经典版-VPN网关”界面所需删除的VPN网关所在行，选择“更多 > 删除”。
   如果所在region已同步上线企业版VPN，在“经典版”界面所需删除的VPN网关所在行，选择“更多 > 删除”。
5. 单击“是”。

2.2 经典版 VPN 连接管理

2.2.1 创建 VPN 连接

操作场景

您需要将VPC中的弹性云服务器和您的数据中心或私有网络连通，创建VPN网关后需要创建VPN连接。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > 经典版 > VPN连接”。
   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。
5. 在“VPN连接”页面，单击“创建VPN连接”。
6. 根据界面提示配置参数，并单击“立即购买”。VPN连接参数请参见**表 VPN连接参数说明**。

表 2-5 VPN 连接参数说明

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	华北-北京四
名称	VPN连接名称。	vpn-001
VPN网关	VPN连接挂载的VPN网关名称。	vpcgw-001
本端子网	本端子网指需要通过VPN访问用户本地网络的VPC子网。支持以下方式设置本端子网： • 选择子网，表示用户数据中心或者私有网络与您选择的子网进行互通。 • 手动输入网段，表示用户数据中心或者私有网络与您配置的网段之间进行互通。 **说明** 多个本端子网不支持子网网段重叠。	192.168.1.0/24， 192.168.2.0/24
远端网关	您的数据中心或私有网络中VPN的公网IP地址，用于与VPC内的VPN互通。	-
远端子网	远端子网指需要通过VPN访问VPC的用户本地子网。远端子网网段不能被本端子网网段覆盖，也不能与本端VPC已有的对等连接网段、专线/云连接的远端子网网段重复。 **说明** 多个远端子网不支持子网网段重叠。	192.168.3.0/24， 192.168.4.0/24

参数	说明	取值样例
预共享密钥	配置在云上VPN连接的密钥，需要与本地网络VPN设备配置的密钥一致。此密钥用于VPN连接协商。 取值范围： ● 取值长度：6~128个字符。 ● 只能包括以下几种字符： – 数字 – 大小写字母 – 特殊符号：包括“~”、“`”、“!”、“@”、“#”、“$”、“%”、“^”、“(”、“)”、“-”、“_”、“+”、“=”、“[”、“]”、“{”、“}”、“|”、"\"、";"、":"、"/"、“:”和“;”	Test@123
确认密钥	再次输入预共享密钥。	Test@123
高级配置	● 默认配置。 ● 已有配置。 ● 自定义配置：包含IKE策略和IPsec策略，用于指定VPN隧道加密算法。相关配置说明请参见**表 IKE策略**和**表 IPsec策略**。	自定义配置

表 2-6 IKE 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： ● MD5（此算法安全性较低，请慎用） ● SHA1（此算法安全性较低，请慎用） ● SHA2-256 ● SHA2-384 ● SHA2-512 默认配置为：SHA2-256。	SHA2-256

参数	说明	取值样例
加密算法	加密算法，支持的算法： ● AES-128 ● AES-192 ● AES-256 ● 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128
DH算法	Diffie-Hellman密钥交换算法，支持的算法： ● Group 1（此算法安全性较低，请慎用） ● Group 2（此算法安全性较低，请慎用） ● Group 5（此算法安全性较低，请慎用） ● Group 14 ● Group 15 ● Group 16 ● Group 19 ● Group 20 ● Group 21 默认配置为：Group 14。	Group 14
版本	IKE密钥交换协议版本，支持的版本： ● v1（有安全风险不推荐） ● v2 默认配置为：v2。	v2
生命周期（秒）	安全联盟（SA—Security Association）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：86400。	86400

表 2-7 IPsec 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： ● SHA1（此算法安全性较低，请慎用） ● MD5（此算法安全性较低，请慎用） ● SHA2-256 ● SHA2-384 ● SHA2-512 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法： ● AES-128 ● AES-192 ● AES-256 ● 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128
PFS	PFS（Perfect Forward Secrecy）即完美前向安全功能，用来配置IPsec隧道协商时使用。 PFS组支持的算法： ● DH group 1（此算法安全性较低，请慎用） ● DH group 2（此算法安全性较低，请慎用） ● DH group 5（此算法安全性较低，请慎用） ● DH group 14 ● DH group 15 ● DH group 16 ● DH group 19 ● DH group 20 ● DH group 21 默认配置为：DH group 14。	DH group 14

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

说明

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

以下算法安全性较低，请慎用：

- **认证算法：**SHA1、MD5。
- **加密算法：**3DES。
- **DH算法：**Group 1、Group 2、Group 5。

7. 单击“提交”。
8. 因为隧道的对称性，还需要在您自己数据中心的路由器或者防火墙上进行IPsec VPN隧道配置。

2.2.2 查看已创建的 VPN 连接

操作场景

用户创建VPN连接后，可以查看已创建的VPN连接。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > 经典版 > VPN连接”。

   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。单击“VPN连接”页签。
5. 在“VPN连接”页面的VPN列表中，查看VPN连接信息，也可以在VPN连接所在行，单击“操作”列的“策略详情”，查看该VPN连接对应的IKE策略和IPsec策略详情。

2.2.3 修改已创建的 VPN 连接

操作场景

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

注意

修改VPN连接高级配置时，有流量中断风险，请谨慎操作。

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

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > 经典版 > VPN连接”。

   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。单击“VPN连接”页签。
5. 在“VPN连接”界面所需修改的VPN连接所在行，单击“修改”。
6. 根据界面提示配置参数。

   说明

   VPN网关名称只能由中文、英文字母、数字、下划线、中划线、点组成。
7. 单击“确定”。

2.2.4 删除 VPN 连接

操作场景

当无需使用VPN网络、需要释放网络资源时，可删除VPN连接。

当购买的VPN网关计费模式为按需时，删除最后一个VPN连接时，会同时删除绑定的VPN网关。

操作步骤

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

   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。单击“VPN连接”页签。

5. 在“VPN连接”界面所需删除的VPN连接所在行，选择“更多 > 删除”。
6. 单击“是”。

2.3 经典版 VPN 管理（墨西哥城一/圣保罗一）

2.3.1 购买 VPN（墨西哥城一/圣保罗一）

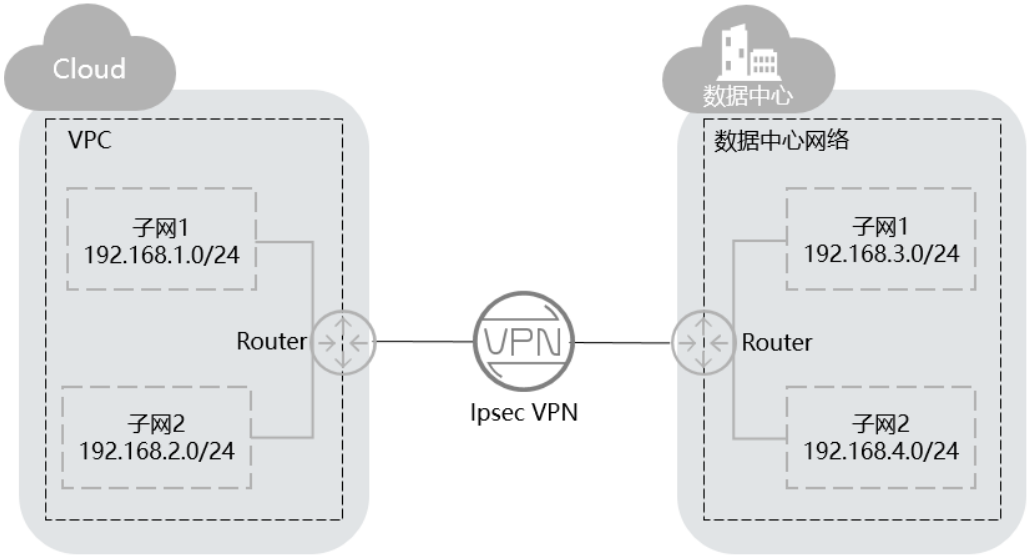
简介

默认情况下，在Virtual Private Cloud (VPC) 中的弹性云服务器无法与您自己的数据中心或私有网络进行通信。如果您需要将VPC中的弹性云服务器和您的数据中心或私有网络连通，可以启用虚拟专用网络功能。此操作您需要在VPC中创建VPN并更新安全组规则。

简单的 IPsec VPN 内网对连拓扑说明

如图2-1所示，假设您在云中已经申请了VPC，并申请了2个子网（192.168.1.0/24，192.168.2.0/24），您在自己的数据中心Router下也有2个子网（192.168.3.0/24，192.168.4.0/24）。您可以通过VPN使VPC内的子网与数据中心的子网互相通信。

图 2-1 IPsec VPN



支持点到点VPN（Site-to-Site VPN），可实现VPC子网和用户数据中心局域网互访。在建立IPsec VPN前，请确认拟开通VPN的用户数据中心满足以下3个条件：

1. 用户数据中心有支持标准IPsec协议的设备。
2. 上述设备可以分配独立的公网IP（NAT IP也支持）。
3. VPC子网和用户数据中心子网不冲突，用户数据中心子网到上述设备可达。

满足以上条件后，配置IPsec VPN时，需要保证两端IKE策略以及IPsec策略配置一致，两端子网互为镜像。

配置完成后，需要通过私网数据流触发VPN协商。

操作场景

通过执行该任务，您可以创建VPN，以便在您的数据中心与云服务之间建立一条保密而安全的通信隧道。

前置条件

- 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
- 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“ “网络” > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络”。
   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。
5. 在“虚拟专用网络”界面，单击“购买VPN”。
   如果所在region已同步上线企业版VPN，在“经典版”界面，单击“购买VPN”。
6. 根据界面提示配置参数，并单击“立即购买”。
   参数说明如**表2-8**、**表2-9**、**表2-10**所示。

表 2-8 基本参数

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	墨西哥城一
计费模式	VPN支持按需计费。	按需计费
名称	VPN名称。	VPN-001
VPC	VPC的名称。	VPC-001
本端子网	本端子网指需要通过VPN访问用户本地网络的VPC子网。	192.168.1.0/24，192.168.2.0/24
远端网关	您的数据中心或私有网络中VPN的公网IP地址，用于与VPC内的VPN互通。	-
远端子网	远端子网指需要通过VPN访问VPC的用户本地子网。远端子网网段不能被本端子网网段覆盖，也不能与本端VPC已有的对等连接网段重合。	192.168.3.0/24，192.168.4.0/24

参数	说明	取值样例
预共享密钥	配置在云上VPN连接的密钥，需要与本地网络VPN设备配置的密钥一致。此密钥用于VPN连接协商。 取值范围：6~128位。	Test@123
确认密钥	再次输入预共享密钥。	Test@123
高级配置	• 默认配置。 • 自定义配置：自定义配置IKE策略和IPsec策略。相关配置说明请参见表2-9和表2-10。	自定义配置
标签	“高级配置”中，选择“标签”。	-

表 2-9 IKE 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： • MD5（此算法安全性较低，请慎用） • SHA1（此算法安全性较低，请慎用） • SHA2-256 • SHA2-384 • SHA2-512 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法： • AES-128 • AES-192 • AES-256 • 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128

参数	说明	取值样例
DH算法	Diffie-Hellman密钥交换算法，支持的算法： ● 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 ● Group 15 ● Group 16 ● Group 19 ● Group 20 ● Group 21 默认配置为：Group 14。	Group 14
版本	IKE密钥交换协议版本，支持的版本： ● v1（v1版本安全性较低，如果用户设备支持v2版本，建议选择v2） ● v2 默认配置为：v2。	v2
生命周期（秒）	安全联盟（SA—Security Association）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：86400。	86400
协商模式	选择IKE策略版本为“v1”时，可以配置协商模式，取值支持Main、Aggressive。 默认配置为：Main	Main

表 2-10 IPsec 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： ● SHA1（此算法安全性较低，请慎用） ● MD5（此算法安全性较低，请慎用） ● SHA2-256 ● SHA2-384 ● SHA2-512 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法： ● AES-128 ● AES-192 ● AES-256 ● 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128
PFS	PFS（Perfect Forward Secrecy）即完美前向安全功能，用来配置IPsec隧道协商时使用。 PFS组支持的算法： ● Disable ● DH group 1（此算法安全性较低，请慎用） ● DH group 2（此算法安全性较低，请慎用） ● DH group 5（此算法安全性较低，请慎用） ● DH group 14 ● DH group 15 ● DH group 16 ● DH group 19 ● DH group 20 ● DH group 21 默认配置为：DH group 14。	DH group 14

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

说明

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

以下算法安全性较低，请慎用：

- **认证算法：**SHA1、MD5。
- **加密算法：**3DES。
- **DH算法：**Group 1、Group 2、Group 5。

7. 提交申请。

   创建成功后云为该IPsec VPN分配一个公网出口IP地址。该地址为VPN页面中，已创建的VPN的本端网关地址。在您自己数据中心配置对端隧道时，远端网关需要配置为该IP地址。

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

2.3.2 查看已购买 VPN

操作场景

用户购买VPN后，可以查看已购买的VPN。

操作步骤

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

   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。

5. 在“虚拟专用网络”界面，即可看到已购买的VPN。
   如果所在region已同步上线企业版VPN，在“经典版”界面，即可看到已购买的VPN。
   其中VPN的状态信息如表2-11所示。

   表 2-11 VPN 状态

状态	说明
正常	当VPN创建成功并已经和用户用户数据中心正常连接时，显示此状态。
未连接	当VPN创建成功，但未和用户用户数据中心连接时，显示此状态。
创建中	当系统正在创建VPN时，显示此状态。
更新中	当系统正在更新VPN信息时，显示此状态。
删除中	当系统正在删除VPN时，显示此状态。
异常	异常情况下，显示此状态。
冻结	VPN资源被冻结时，显示此状态。

2.3.3 修改已购买 VPN

操作场景

当创建的VPN网络信息和VPC网络有冲突或需要根据最新网络环境调整时，可通过修改VPN信息的方式进行调整。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络”。
   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。
5. 在“虚拟专用网络”界面所需修改的VPN所在行，单击“修改”。
   如果所在region已同步上线企业版VPN，在“经典版”界面所需修改的VPN所在行，单击“修改”。
6. 根据界面提示配置参数。
7. 单击“确定”。

2.3.4 删除 VPN

操作场景

当无需使用VPN网络、需要释放网络资源时，可删除VPN。

操作步骤

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

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

   如果所在region已同步上线企业版VPN，在“经典版”界面所需删除的VPN所在行，单击“删除”。
6. 单击“是”。

2.4 经典版 VPN 费用管理

2.4.1 按需按带宽转包年/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。

  计费方式以实际region购买界面为准。
- 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

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

   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。单击“VPN网关”页签。
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。
8. 单击“去支付”，进入支付界面。
9. 在支付界面，确认订单信息，选择优惠和付款方式。
10. 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。

2.4.2 按需按带宽进行带宽升配或降配

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进行升配或降配。

计费方式以实际region购买界面为准。

操作步骤

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

   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。单击“VPN网关”页签。
5. 在VPN网关列表页面，选择目标VPN网关所在行。
6. 在目标VPN网关所在行的“操作”列，选择“更多 > 修改带宽 ”，进入修改带宽页面。
7. 选择目标带宽大小。
8. 单击“提交”，完成按需按带宽进行带宽升配或降配。

   带宽调整后，将在下个计费周期生效。

2.4.3 按需按带宽与按需按流量相互转换

前提条件

计费方式选择为按需计费。即当前支持按需按带宽与按需按流量的按需计费方式相互转换。

计费方式以实际region购买界面为准。

操作步骤

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

   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。单击“VPN网关”页签。
5. 在VPN网关列表页面，选择目标VPN网关所在行。
6. 在目标VPN网关所在行的“操作”列，选择“更多 > 修改带宽 ”，进入修改带宽页面。
7. 在修改带宽页面，选择“变更规格 > 按带宽计费”。
8. 单击“提交”，完成按需按流量转按需按带宽。

2.4.4 按需按流量转包年/包月

前提条件

计费方式选择为按流量计费。即当前支持按流量的按需计费方式转包年/包月。

计费方式以实际region购买界面为准。

操作步骤

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

   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。单击“VPN网关”页签。
5. 在VPN网关列表页面，选择目标VPN网关所在行。
6. 在目标VPN网关所在行的“操作”列，选择“更多 > 修改带宽 ”，进入修改带宽页面。
7. 在修改带宽页面，选择“变更规格 > 按带宽计费”。
8. 单击“提交”，完成按需按流量转按需按带宽。
9. 返回VPN网关列表页面，再次选择目标VPN网关所在行。
10. 在目标VPN网关所在行的“操作”列，选择“更多 > 转包年/包月 ”。
11. 单击“确定”，进入按需转包年/包月页面。
12. 选择续费时长，单击“去支付”。
13. 选择支付方式，单击“确认付款”。

3 终端入云 VPN

3.1 终端入云 VPN 网关管理

3.1.1 创建 VPN 网关

场景描述

如果您需要使用终端设备远程接入VPC，使用户可以安全地访问VPC中部署的应用或服务，在使用终端入云VPN之前，需要创建VPN网关。

约束与限制

用户最多可创建50个VPN网关。

前提条件

- 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
- 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“终端入云VPN网关”进入终端入云VPN网关页面，单击“创建终端入云VPN网关”。

步骤6 根据界面提示配置参数，单击“立即购买”并完成支付。

VPN网关参数请参见**表3-1**。

表 3-1 VPN 网关参数说明

参数	说明	取值样例
计费模式	支持“包年/包月”和“按需计费”两种模式。 支持“按需计费”。	包年/包月 按需计费
区域	选择靠近您所在地域的区域可以降低网络时延，从而提高访问速度。 不同区域的资源之间网络不互通。	*请根据实际需要进行选择*
名称	输入VPN网关的名称。	p2c-vpngw-001
虚拟私有云	选择虚拟私有云VPC信息。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在3个及以上可分配的IP地址。	192.168.66.0/24
规格	仅支持专业型1。 详细规格差异请参见**规格介绍**。	专业型1
可用区	可用区是指在同一地域内，电力和网络互相独立的物理区域。在同一VPC网络内可用区与可用区之间内网互通，可用区之间能做到物理隔离。 ● 当存在两个及以上可用区时，必须选择两个可用区。 部署在两个可用区的VPN网关具备更高的可用性。建议您根据VPC内资源所在的可用区选择网关的可用区。 ● 当仅存在一个可用区时，可选择此可用区创建VPN网关。	可用区1、可用区2
连接数	VPN网关最多支持10个免费的VPN连接，提供可选连接数规格，支持用户自定义。 **说明** 自定义连接数为10，是包含VPN网关默认提供10个免费的VPN连接数。	10
EIP	用于VPN网关和客户端进行网络连接。 ● 现在创建：购买新EIP，新购买EIP的计费模式为包周期。 ● 使用已有：使用已有EIP，仅支持使用独享带宽的EIP。 **说明** 使用已有EIP时，已有EIP的计费模式可以为按需，也可以为包年/包月。	现在创建

参数	说明	取值样例
弹性公网IP类型	仅“EIP”选择“现在创建”时需要配置。 全动态BGP：可以根据设定的寻路协议实时自动优化网络结构，以保持客户使用的网络持续稳定、高效。 弹性公网IP类型的详细介绍请参见**什么是弹性公网IP**。	全动态BGP
带宽大小	仅“EIP”选择“现在创建”时需要配置。 EIP对应带宽大小，单位：Mbit/s。 • 所有使用该EIP创建的VPN连接均会分摊占用该EIP的带宽大小，所有VPN连接的带宽总和不能超过该EIP的带宽大小。 当网络流量超过EIP的带宽大小时，有可能造成网络拥塞导致VPN连接中断，请提前做好带宽规划。 • 支持在云监控中配置告警规则对带宽进行监控。 • 支持用户在允许的带宽范围内自定义带宽大小。 • 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。	20 Mbit/s
带宽名称	仅“EIP”选择“现在创建”时需要配置。 EIP对应带宽对象的名称。	p2c-vpngw-bandwidth1
高级设置/标签	• VPN服务的资源标签，包括键和值，最大可以创建20对标签。 • 标签设置时，可以选择预定义标签，也可以自定义创建。 • 预定义标签可以通过单击“查看预定义标签”进行查看。	-
购买时长	在账户余额充足场景下，如果勾选“自动续费”功能，系统会在当前服务购买时长到期后自动进行续费。 • 按月购买场景，自动续费周期为一个月。 • 按年购买场景，自动续费周期为一年。	6

----结束

3.1.2 修改 VPN 网关

场景描述

用户创建VPN网关后，可以对VPN网关基本信息进行修改，包括名称和带宽。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“终端入云VPN网关”进入“终端入云VPN网关”页面。

- 修改VPN网关名称：单击VPN网关名称右侧的按钮进行修改，单击“确认”。
- 修改绑定EIP带宽：单击VPN网关名称，在“基本信息 > 弹性公网IP”区域，单击“带宽大小”右侧的“修改”并完成费用确认。

----结束

3.1.3 查看 VPN 网关

场景描述

用户创建VPN网关后，可以对已创建的VPN网关的相关信息进行查看。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“终端入云VPN网关”进入“终端入云VPN网关”页面。

步骤6 单击VPN网关的名称，查看VPN网关详情。

- 客户端认证类型为证书认证时，可以查看如下详情。
  - 基本信息：可查看VPN网关基本信息和弹性公网IP基本信息。
  - 服务端：可查看服务端基本信息、认证信息、高级配置。
  - 连接：可查看与服务端已建立的VPN连接信息，包括ID、虚拟地址、实际地址、上线时间、入方向字节数、出方向字节数、入向数据包、出向数据包。
  - 标签：可查看并管理VPN网关已创建的标签标签键和标签值。
- 客户端认证类型为口令认证（本地）时，可以查看如下详情。
  - 基本信息：可查看VPN网关基本信息和弹性公网IP基本信息。
  - 服务端：可查看服务端基本信息、认证信息、高级配置。
  - 用户管理：可查看已创建的用户和用户组。
  - 访问策略：可查看网关策略信息，包括名称/ID、用户组、目的网段、描述、更新时间。

- 连接：可查看与服务端已建立的VPN连接信息，包括ID、虚拟地址、实际地址、用户名称、上线时间、入方向字节数、出方向字节数、入向数据包、出向数据包。
- 标签：可查看并管理VPN网关已创建的标签标签键和标签值。

----结束

3.1.4 退订 VPN 网关

场景描述

当用户无需使用VPN网关时，可以退订VPN网关。

约束与限制

- 在VPN网关状态处于“创建中”、“更新中”、“退订中”等状态时，不能进行VPN网关退订操作。
- 如果VPN网关绑定的EIP计费模式为按需，退订VPN网关时会同步解绑EIP。解绑后弹性公网IP继续保留，若不再使用可在网关退订后释放。
- 退订VPN网关会导致关联的VPN连接立即中断。
- 退订VPN网关时，自生成的服务端证书也会自动删除。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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“更多 > 退订”。

步骤6 根据界面提示，完成退订操作。

----结束

3.1.5 绑定弹性公网 IP

场景描述

用户根据需要为已创建的VPN网关绑定EIP。

操作步骤

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 单击“终端入云VPN网关”进入终端入云VPN网关页面。

步骤5 在终端入云VPN网关页面，选择目标VPN网关所在行，单击操作列的“更多 > 绑定EIP”。

步骤6 根据界面提示，选择需要绑定的EIP，单击确定。

说明

更新弹性公网IP后请重新下载客户端配置。

----结束

3.1.6 解绑弹性公网 IP

场景描述

用户创建VPN网关后，可以解绑已关联的弹性公网IP。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“终端入云VPN网关”进入“终端入云VPN网关”页面。

步骤6 在终端入云VPN网关页面，选择目标VPN网关所在行，单击操作列的“更多 > 解绑EIP”。

步骤7 根据界面提示，完成解绑操作。

说明

未绑定VPN网关的弹性公网IP会继续计费，如果不再使用建议释放。

----结束

3.1.7 按标签搜索 VPN 网关

场景描述

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

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

前提条件

已为VPN资源添加标签，详细操作请参见**为云资源添加标签**。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“终端入云VPN网关”进入“终端入云VPN网关”页面。

步骤6 在“终端入云VPN网关”页面，单击搜索框“选择属性筛选，或输入关键字搜索”，选择“资源标签 ”，添加筛选条件标签键值。

- 此查询功能仅支持选择标签列表中已存在的键和值。
- 支持最多20个不同标签的组合搜索。如果输入多个标签，则不同标签之间为“或”的关系。
- 支持标签和其他条件进行组合搜索。标签和其他搜索条件组合的搜索也是“或”的关系。

----结束

3.1.8 升级网关实例

升级概述

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

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

当升级状态处于“请确认是否完成升级”时，用户可以根据实际需要进行回退操作。

约束与限制

如果VPN网关、EIP或共享带宽的计费模式为包周期，只有当距离到期时间超过1天时，才能进行网关实例的升级和回退操作。

升级影响

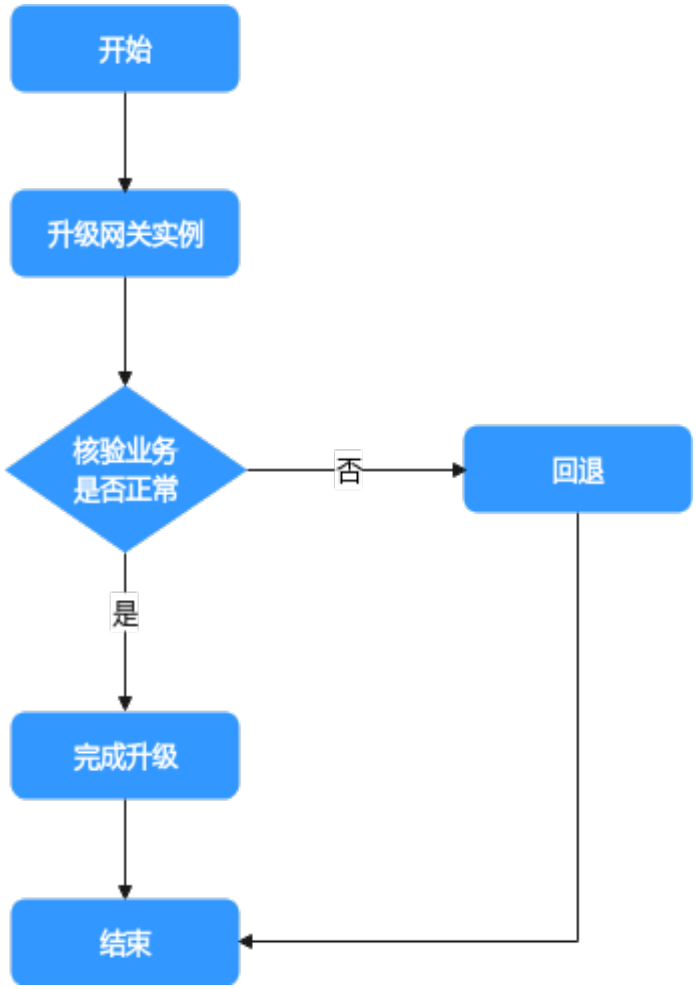
- 升级中VPN连接会出现中断，中断时间大约为10分钟。
- 升级中VPN网关以及其VPN连接均无法操作。

回退机制

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

操作步骤

图 3-1 升级流程示意图



步骤1 升级网关实例。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 单击“终端入云VPN网关”，进入终端入云VPN网关界面。
5. 选择目标VPN网关，单击操作列的“升级网关实例”。
6. 在弹窗中了解升级影响和回退机制，勾选“我已知晓以上升级须知”后，单击确定。
7. 查看升级状态。实例升级过程中，可以在VPN网关列表页的状态列单击查看任务，查看升级进展。
   - 如果实例升级成功，VPN网关的状态会刷新为“请确认是否完成升级”，进入步骤2。
   - 如果实例升级失败，会自动回滚。可以在VPN网关列表页的右上方，查看失败信息。

步骤2 核验业务。

1. 核验业务正常，单击操作列的“完成升级”。

   须知

   单击“完成升级”后，升级任务无法回退，请谨慎选择。

2. 核验业务异常，单击操作列的“回退”，请**提交工单**联系华为工程师。

----结束

3.1.9 删除 VPN 网关

场景描述

当用户无需使用VPN网关时，可以删除VPN网关。

约束与限制

- 在VPN网关状态处于“创建中”、“更新中”、“删除中”等状态时，不能进行VPN网关删除操作。
- 删除VPN网关会导致关联的VPN连接立即中断。
  VPN网关绑定的按需计费的弹性公网IP将会自动释放。
- 删除VPN网关时，自生成的服务端证书也会自动删除。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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“更多 > 删除”。

步骤6 根据界面提示，单击“一键输入”，完成删除操作。

----结束

3.2 终端入云 VPN 服务端管理

3.2.1 配置服务端

场景描述

服务端提供配置管理和连接认证，终端入云VPN网关创建完成后，需要对服务端进行相关配置。

前提条件

请确认服务端关联的VPN网关已创建成功。

约束与限制

- 只有VPN网关处于“正常”状态时，才能进行服务端配置操作。
- 一个VPN网关仅支持关联一个服务端。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“终端入云VPN网关”，进入“终端入云VPN网关”页面。

步骤6 单击目标VPN网关操作列的“配置服务端”，或者单击目标VPN网关名称进入详情页配置服务端。

步骤7 根据界面提示配置参数。

服务端配置参数请参见表3-2。

表 3-2 服务端参数说明

区域	参数	说明	取值样例
基本信息	本端网段	本端网段是客户端通过终端入云VPN网关访问的目标网络的地址段。本端网段可以是华为云VPC的网段，或与华为云VPC互联网络的网段。 最多可指定20个本端网段。本端网段的全0配置，暂不开放支持。本端网段的限制网段为0.0.0.0/8，224.0.0.0/4，240.0.0.0/4，127.0.0.0/8，不能与这些特殊网段重叠或冲突。 ● 选择子网： 选择本VPC子网信息。 ● 输入网段： 可以输入本VPC下的子网信息；也可以输入与本VPC建立了对等网络的VPC子网信息。 **说明** 本端网段修改后，客户端需要重新连接。	192.168.0.0/24

区域	参数	说明	取值样例
	客户端网段	客户端网段是分配给客户端虚拟网卡地址的网段，不能与本端网段重叠，不能与网关所在VPC的路由表内路由重叠。当客户端连接网关时，会从中分配一个IP地址给客户端使用。 客户端网段需要满足点分十进制/掩码格式，掩码位数在16~26之间。系统在为每个客户端分配IP地址时，需要划分出一个子网掩码为30的子网段，用以保证网络通信正常。因此，请确保您指定的客户端网段所包含的IP地址个数是VPN网关连接数的4倍及以上。 不同VPN连接数建议的客户端网段请参见**表3-3**。 **说明** • 客户端网段不能包含100.64.0.0/10、100.64.0.0/12和214.0.0.0/8等预留网段。不同region的预留网段不同，实际使用以控制台显示为准。 如果需要使用100.64.0.0/10或100.64.0.0/12，请**提交工单**申请。 • 客户端网段修改后，客户端需要重新连接。	172.16.0.0/16
	隧道类型	SSL协议是一种传输层安全协议，用于构建客户端和服务端之间的安全通道。 OpenVPN（SSL），不支持修改。	OpenVPN（SSL）
认证信息	服务端证书	服务端证书是服务端使用的SSL证书，客户端会基于此证书验证服务端的身份。 • 服务自签名证书。 • 选择已有证书。 – 上传证书：单击下拉框最下方的“上传证书”，跳转至云证书与管理服务。按照界面提示上传服务端证书，详细步骤请参见**上传已有SSL证书**。 – 推荐使用强密码算法的证书，如RSA3072/4096。 **说明** 用户在完成服务端配置后，在云证书与管理服务中删除了引用的服务端证书，并不影响服务端证书的可用性。	*请根据实际需要进行选择*

区域	参数	说明	取值样例
	客户端认证类型	客户端认证类型是服务端验证客户端身份的方式。支持“证书认证”、“口令认证（本地）”、“IAM认证”和“联邦认证”四种方式。 ● 选择“客户端认证类型 > 证书认证”。单击“上传CA证书”，以文本格式打开CA证书PEM格式的文件，将证书内容复制到“上传CA证书”的“内容”文本框内。最多支持添加10个客户端CA证书。 推荐使用强密码算法的证书，如RSA3072/4096。RSA2048加密算法的证书存在风险，请慎用。 证书验证通过后，您可以在列表中查看CA证书基本信息，包含名称、序列号、签名算法、颁发者、使用者、过期时间。 ● 选择“客户端认证类型 > 口令认证（本地）”。 客户端认证类型使用口令认证时，需要创建用户。 创建用户时，默认可以访问云上全部资源。如果需要自定义可访问范围，请参考**创建用户/用户组**和**创建访问策略**。 **说明** default访问策略适用于default用户组中的所有用户。如果不需要default访问策略，可以将其删除，自定义创建访问策略。 ● 选择“客户端认证类型 > IAM认证”。当认证类型为IAM认证时，用户需要创建用户组，且用户组中的用户要具有VPN SSOAccessPolicy权限。 ● 选择“客户端认证类型 > 联邦认证”。当客户端认证类型为联邦认证时，用户需要执行以下操作： – 创建用户组，将用户组授予VPN SSOAccessPolicy权限。 – 配置身份提供商，在配置过程中设置身份转换规则。 在创建身份提供商时，目前仅支持创建基于SAML协议的虚拟用户SSO的身份提供商。 如何配置虚拟用户SSO类型的身份提供商，请参见**基于SAML协议的虚拟用户SSO**。 **说明** 当客户端认证类型为“IAM认证”和“联邦认证”时，不支持使用区域子项目中的网关资源。关于子项目的详细介绍，请参考**项目管理**。	*请根据实际需要进行选择*

区域	参数	说明	取值样例
高级配置	协议	终端入云VPN连接使用的协议。 TCP（默认）	TCP
	端口	终端入云VPN连接使用的端口。 ● 443（默认） ● 1194	443
	加密算法	终端入云VPN连接使用的加密算法。 ● AES-128-GCM（默认） ● AES-256-GCM	AES-128-GCM
	认证算法	终端入云VPN连接使用的认证算法。 ● 加密算法为AES-128-GCM时，对应认证算法为SHA256。 ● 加密算法为AES-256-GCM时，对应认证算法为SHA384。	SHA256
	是否压缩	是否对传输数据进行压缩处理。 默认不压缩，不支持修改。	否
	域名访问	支持开启和关闭域名访问。 ● 开启 配置DNS服务器地址，客户端可以通过域名访问云上网络。具体如何部署DNS服务器，请参考**云解析服务 DNS**。 配置合法的DNS服务器地址，取值如下： – 非0.0.0.0。 – 非loopback地址，取值范围是127.0.0.0 ~ 127.255.255.255。 – 非组播地址，取值范围是224.0.0.0 ~ 239.255.255.255。 – 非0开头与0结尾。 – 输入的DNS地址重复检查。 – 非255.255.255.255。 ● 关闭	开启 *请根据实际DNS服务器地址填写*

表 3-3 建议的客户端网段

VPN连接数	建议的客户端网段
10	子网掩码位数小于或等于26的网段。 例如：10.0.0.0/26、10.0.0.0/25。

VPN连接数	建议的客户端网段
20	子网掩码位数小于或等于25的网段。 例如：10.0.0.0/25、10.0.0.0/24。
50	子网掩码位数小于或等于24的网段。 例如：10.0.0.0/24、10.0.0.0/23。
100	子网掩码位数小于或等于23的网段。 例如：10.0.0.0/23、10.0.0.0/22。
200	子网掩码位数小于或等于22的网段。 例如：10.0.0.0/22、10.0.0.0/21。
500	子网掩码位数小于或等于21的网段。 例如：10.0.0.0/21、10.0.0.0/20。

步骤8 单击“确定”。

----结束

3.2.2 查看服务端

场景描述

服务端配置完成后，您可以查看服务端配置。

前提条件

请确认服务端配置已完成。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

- 基本信息：可查看服务端ID、本端网段、客户端网段、隧道类型、状态。
- 认证信息：可查看服务端证书和客户端认证类型。
- 高级配置：可查看协议、端口、加密算法、认证算法、是否压缩和域名访问。

----结束

3.2.3 修改服务端

场景描述

您可以对服务端配置进行修改。

说明

- 如果您设置了指定客户端IP，再修改服务端的客户端网段，客户端需要重新连接，用户的指定IP会被清理。
- 如果您修改了高级配置中的协议、端口等参数，需要重新下载并导入新的客户端配置文件，参数修改才能生效。

操作须知

- 修改端口、加密算法，会导致客户端断开后无法重新连接，需要下载新的客户端配置，使用新的客户端配置文件重新接入。
- 增删改VPN网关本端网段、VPN连接的客户端网段、客户端认证类型和访问策略配置等操作可能会导致网络中断，请谨慎操作。

修改服务端操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“终端入云VPN网关”页签，单击目标VPN网关所在行操作列的“查看服务端”。

步骤6 修改服务端配置。

- 单击“基本信息”右侧的按钮对本端网段和客户端网段进行修改，单击“确定”。
- 单击“服务端证书”操作列的“更换”，对服务端证书进行修改，单击“确定”。
- 单击“客户端认证类型”右侧的按钮，对客户端认证类型进行修改，单击“确定”。
- 单击“高级配置”右侧的按钮，对端口、加密算法和域名访问进行修改，单击“确定”。

注意

DNS服务器地址修改后，客户端需要重新连接才能生效。

----结束

修改服务端证书操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 选择“终端入云VPN网关”页签，在“终端入云VPN网关”界面目标VPN网关所在行操作列，单击“查看服务端”进入服务端配置界面。

步骤6 在“服务端”界面，单击服务端证书操作列的“更换”，进入“更换服务端证书”弹窗页面。

步骤7 选择“服务端证书”，单击“确定”。

注意

由服务自签名证书切换到已有证书后，不支持再切换回服务自签名证书。

更换服务端证书，会导致客户端断开后无法重新连接，需要下载新的客户端配置，使用新的客户端配置文件重新接入。

----结束

修改客户端认证类型操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 选择“终端入云VPN网关”页签，在“终端入云VPN网关”界面目标VPN网关所在行操作列，单击“查看服务端”进入服务端配置界面。

步骤6 修改客户端认证类型有以下四种场景。

注意

修改认证类型后，原有连接都将中断。

- 将口令认证（本地）修改为其他认证类型。
  a. 删除口令认证对应的用户、用户组和访问策略。
  b. 单击“口令认证（本地）”右侧的按钮
  c. 在修改客户端认证类型的弹窗中，选择要修改的认证类型。

d. 单击“确定”。

- 将“证书认证”修改为其他认证类型。
  a. 删除证书认证对应的CA证书。
  b. 单击“证书认证”右侧的按钮。
  c. 在修改客户端认证类型的弹窗中，选择要修改的认证类型。
  d. 单击“确定”。

  说明

  口令认证会自动生成名称为default的访问策略，default访问策略适用于default用户组中的所有用户。

- 将IAM认证修改为其他认证类型。
  a. 单击“IAM认证”右侧的按钮。
  b. 在修改客户端认证类型的弹窗中，选择要修改的认证类型。
  c. 单击“确定”。
- 将联邦认证修改为其他认证类型。
  a. 单击“联邦认证”右侧的按钮。
  b. 在修改客户端认证类型的弹窗中，选择要修改的认证类型。
  c. 单击“确定”。

----结束

3.2.4 上传服务端证书

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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“配置服务端”。

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”，根据界面提示填写相关信息。

上传证书参数请参见**表 上传国际标准证书参数说明**。

表 3-4 上传国际标准证书参数说明

参数	说明
证书标准	选择国际标准证书。
证书名称	用户自定义。
企业项目	将上传的SSL证书分配至对应的企业项目中。
证书文件	以文本编辑器（如Notepad++）打开待上传证书里的CER或CRT格式的文件，将证书内容复制到此处。 按照“服务端证书--CA证书”的顺序依次排列上传。 **说明** 用户如果没有现成的证书，可以采用自签发的方式生成证书，然后上传。证书文件请参考**通过Easy-RSA自签发证书（服务端和客户端共用CA证书）**。 上传证书文件格式如**图 证书上传格式**。
证书私钥	以文本编辑器（如Notepad++）打开待上传证书里的KEY格式的文件，将私钥内容复制到此处。 仅上传服务端证书私钥。 上传证书私钥格式如**图 证书上传格式**。

图 3-2 证书上传格式

说明

服务端证书的CN必须是域名格式。

步骤8 单击确定，完成上传证书。

步骤9 查看证书列表，确认证书状态为“托管中”。

----结束

3.2.5 修改服务端证书

操作须知

更换服务端证书，会导致客户端断开后无法重新连接，需要下载新的客户端配置，使用新的客户端配置文件重新接入。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 在“服务端”界面，选择服务端证书操作列，单击“更换”，进入“更换服务端证书”弹窗页面。

步骤7 选择“服务端证书”，单击确定。

注意

- 由服务自签名证书切换到已有证书后，不支持再切换回系统自生成。
- 更换服务端证书，会导致客户端断开后无法重新连接，需要下载新的客户端配置，使用新的客户端配置文件重新接入。

----结束

3.2.6 上传客户端 CA 证书

约束与限制

仅“客户端认证类型””选择“证书认证 ”时需要配置。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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“配置服务端”或“查看服务端”。

步骤6 在“服务端”界面，在“客户端认证类型”下拉选项中选择“证书认证 ”，单击“上传CA证书”。

步骤7 根据界面提示填写相关信息。

表 3-5 上传 CA 证书参数说明

参数	说明	取值样例
名称	支持修改。	ca-cert-server
内容	以文本编辑器（如Notepad++）打开签名证书PEM格式的文件，将证书内容复制到此处。 **说明** • 推荐使用强密码算法的证书，如RSA3072/4096。 • RSA2048加密算法的证书存在风险，请慎用。	-----BEGIN CERTIFICATE----- MIIDoTCCAomgAwIBAgIUZAxA/2WlDFidbH9QfedbwYHrmQQwDQYJKoZIhvcNAQEL BQAwYDELMAkGA1UEBhMCQ04xCzAJBgNVBAgMAkJKMQswCQYDVQQHDAJCSjEPMA0G -----END CERTIFICATE-----

步骤8 单击确定。

说明

最多支持添加10个客户端CA证书。

----结束

3.2.7 删除客户端 CA 证书

约束与限制

仅“客户端认证类型””选择“证书认证 ”，且已上传CA证书时可以删除。

操作须知

删除该CA证书后，相关的客户端无法再正常连接，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 在“服务端”界面，选择客户端CA证书的操作列，单击“删除”。

步骤7 在“删除CA证书”的弹窗中，单击确定。

----结束

3.2.8 创建用户/用户组

约束与限制

- 仅“客户端认证类型””选择“口令认证（本地）”时需要配置。
- 每个用户最多同时建立5个连接。
- 单个VPN网关支持创建500个用户。

创建用户操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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“配置服务端”或“查看服务端”。

步骤6 在“服务端”界面，选择客户端认证类型“口令认证（本地）”，单击确定。

步骤7 选择“用户管理 > 用户”，单击“创建用户”。

填写参数请参见表3-6。

表 3-6 创建用户参数说明

参数	说明
名称	格式为英文字母、数字、“.”、“_”或“-”，最多包含64个字符。 **说明** 以下名称格式为系统内部预留用户名，请不要使用： • L3SW_（前缀） • link • Cascade • SecureNAT • localbridge • administrator（不区分大小写）
描述	用户自定义。

参数	说明
密码	• 长度范围是8到32个字符。 • 至少包含以下字符中的2种：大写字母、小写字母、数字、特殊字符`~!@#$%^&*()-_=+|[{}];:'",<.>/? 和空格。 • 不能与用户名或倒序的用户名相同。 **说明** 为保障账号安全，建议用户定期修改密码。
确认密码	同“密码”设置参数保持一致。
所属用户组	默认所属用户组为default。
是否指定客户端IP	选择“是否指定客户端IP”的开关。 • 开启 当选择开启时，指定IP会断开使用该IP的连接。 • 关闭 **注意** • 指定IP地址不能与客户端地址池的网关IP重复。 • 指定IP地址必须填写30位掩码网段的第一个主机地址。 • 指定IP地址不能与其他用户指定的IP地址重复。 • 指定IP地址需要在客户端地址池范围内。

步骤8 单击确定。

返回“用户”页签，可以查看用户信息。包括名称/ID、用户组、创建时间和静态IP等。

----结束

说明

添加的用户最大数量为用户购买VPN网关的最大连接数。

创建用户组操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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“配置服务端”或“查看服务端”。

步骤6 在“服务端”界面，选择客户端认证类型“口令认证（本地）”，单击确定。

步骤7 选择“用户管理 > 用户组”，单击“创建用户组”，填写名称和描述，单击确定。

----结束

说明

- 用户组名称要求唯一。
- 用户组数量配置最大为50。
- 目前用户组不支持配额修改。
- 创建用户组后，需配置访问策略才能访问云上资源。

将用户添加到用户组操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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“配置服务端”或“查看服务端”。

步骤6 在“服务端”界面，选择客户端认证类型“口令认证（本地）”，单击确定。

步骤7 将用户添加到用户组的两种方法。

- 从“用户”页签添加用户。
  a. 选择“用户管理 > 用户”，单击“创建用户”。
  b. 根据界面提示配置参数。
  所属用户组选择将要加入的用户组。

  说明

  如果创建用户时未选择所属用户组，可以在对应用户的操作列单击“修改”选择用户组。

  c. 单击确定。
- 从“用户组”页签添加用户。
  a. 选择“用户管理 > 用户组”，单击“创建用户组”，填写名称和描述，单击确定。
  b. 在已创建的用户组所在行，单击操作列的“添加用户”。
  c. 在“添加用户”的弹窗里勾选可选用户并单击 按钮，单击确定。

----结束

3.2.9 修改用户/用户组

约束与限制

仅“客户端认证类型””选择“口令认证（本地）”，且已创建用户/用户组时可以修改。

操作须知

修改所属用户组后，原有连接将中断，请谨慎操作。

修改用户操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 选择“用户管理 > 用户”，选择目标用户所在行，单击操作列“修改”，修改描述、所属用户组和是否指定客户端IP。

当是否指定客户端IP选择开启时，指定IP会断开该用户的所有连接以及使用该IP的连接。

说明

为保障账号安全，建议用户定期修改密码。

----结束

修改用户组操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 选择“用户管理 > 用户组”，选择目标用户组所在行，单击操作列“修改”，修改名称和描述。

注意

default用户组不支持“修改”与“删除”。

----结束

3.2.10 删除用户/用户组

约束与限制

仅“客户端认证类型””选择“口令认证（本地）”，且已创建用户/用户组时可以删除。

操作须知

删除用户后，该用户的连接会中断，无法再连接，请谨慎操作。

删除用户操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 选择“用户管理 > 用户”，选择目标用户所在行，单击操作列的“删除”。

步骤7 在删除用户的弹窗页，单击确定。

----结束

移除用户操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 选择“用户管理 > 用户组”，单击用户组，进入用户列表详情页。

步骤7 选择目标用户所在行，单击操作列的“移除”。

步骤8 在“移除用户”的弹窗页，单击确定。

注意

移除后用户将无法访问云上资源。

----结束

删除用户组操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 选择“用户管理 > 用户组”，选择目标用户组所在行，单击操作列的“删除”。

步骤7 在“删除用户组”的弹窗页，单击确定。

注意

- 删除用户组后，该用户组下的用户将无法访问云上资源。
- default用户组不支持“修改”与“删除”。

----结束

3.2.11 创建访问策略

约束与限制

- 仅“客户端认证类型””选择“口令认证（本地）”时可以配置。
- 单策略目的网段数量：10。
- 访问策略数量最大规格：100。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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“配置服务端”。

步骤6 在“服务端”界面，选择客户端认证类型“口令认证（本地）”，单击“确定”。

步骤7 在“访问策略”页签中，单击“创建策略”。

步骤8 填写名称、目的网段和用户组。

步骤9 单击“确定”。

说明

口令认证会自动生成名称为default的访问策略，default访问策略适用于default用户组中的所有用户。

----结束

3.2.12 修改访问策略

约束与限制

- 仅“客户端认证类型””选择“口令认证（本地）”，且已创建自定义访问策略时可以修改。
- 自动生成的default访问策略，不支持修改。

操作须知

修改访问策略可能会导致网络中断，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 选择“访问策略”，选择目标策略所在行，单击操作列“修改”。修改名称、目的网段、描述、用户组。

步骤7 单击“确定”。

----结束

3.2.13 删除访问策略

约束与限制

仅“客户端认证类型””选择“口令认证（本地）”时，可以删除。

操作须知

删除访问策略后，该策略关联的用户组下的用户将无法访问对应的云上资源，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 选择“访问策略”，选择目标策略所在行，单击操作列“删除”。

步骤7 在“删除策略”的弹窗页，单击“一键输入”。

步骤8 单击“确定”。

----结束

3.2.14 重置用户密码

约束与限制

仅“客户端认证类型””选择“口令认证（本地）”，且已创建用户时可以重置密码。

重置用户密码操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 选择“用户管理 > 用户”，选择目标用户所在行，单击操作列的“重置密码”。

步骤7 在“重置密码”的弹窗页，填写新密码并确认新密码，单击确定。

说明

为保障账号安全，建议用户定期修改密码。

----结束

3.2.15 批量导入用户

约束与限制

- 仅“客户端认证类型”选择“口令认证（本地）”时可以配置。
- 只支持在windows系统网页里操作。
- 单个VPN网关支持创建500个用户。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 选择“用户管理 > 用户”，单击“导入用户”。

步骤7 在弹窗中单击“下载模板”，打开已下载的.xlsx模板文件。

填写模板中的名称、密码、所属用户组名和静态IP等。

说明

如果填写了静态IP列参数，客户端默认使用指定静态IP，不会分配动态IP。

步骤8 单击“选择文件”，上传已填写的模板文件。

当模板内容填写错误时，会提示“文件内容不合法”，需要重新修改已填写的模板文件，修改后，再重新导入文件。

说明

- 上传文件的大小不超过50k。
- 只支持上传.xlsx类型文件（支持Excel 2007及更高版本的.xlsx文件格式）。
- 文件的表头必须与下载的模板表头一致。
  建议不要修改原有的模板内容，否则导入已填写的模板文件后系统将无法识别文件。
- 文件中的用户记录数不超过500。

步骤9 单击“确认”，可批量导入用户。

----结束

3.2.16 批量删除用户

约束与限制

仅“客户端认证类型””选择“口令认证（本地）”时可以配置。

操作须知

删除用户后，该用户的连接会中断，无法再连接，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 选择“用户管理 > 用户”，选择需要删除的用户，单击“删除用户”。

步骤7 在“删除用户”的弹窗页，单击确定。

----结束

3.2.17 查看 VPN 连接

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 单击“连接”页签，可以查看当前连接详情。包括ID、虚拟地址、实际地址、上线时间、操作等。

说明

- 当客户端认证类型是选择“口令认证（本地）”和“联邦认证”时，VPN连接详情中会多一列用户名称。
- 用户名称显示为“FederationUser”可能是未配置身份转换规则，如需显示实际用户，请到身份提供商页面配置。

----结束

3.2.18 断开 VPN 连接

约束与限制

只有VPN网关处于正常状态下，用户才能进行断连操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 单击“连接”页签，选择目标VPN连接所在行，单击操作列的“断开”。

> **⚠ 注意**
>
> 请谨慎断开连接，断开后该VPN客户端将下线。如需限制该客户端重新上线，请重置密码。

步骤7 单击确定，断开连接请求下发成功，稍后生效。

----结束

3.2.19 查看 VPN 连接日志

操作场景

用户在使用VPN日志记录时，可以查询指定连接的日志信息。

前提条件

用户已经开通云日志服务。如何开通云日志服务，请参见**云日志服务**。

操作步骤

- 创建日志组
  a. 登录管理控制台。
  b. 在管理控制台左上角单击 图标，选择区域和项目。
  c. 在页面左上角单击图标，选择“管理与监管 > 云日志服务”。
  d. 创建日志组，如何创建请参见**管理日志组**。
- 创建日志流
  a. 登录管理控制台。
  b. 在管理控制台左上角单击 图标，选择区域和项目。
  c. 在页面左上角单击图标，选择“管理与监管 > 云日志服务”。
  d. 创建日志流，如何创建请参见**管理日志流**。
- 配置连接日志
  a. 登录管理控制台。
  b. 在管理控制台左上角单击 图标，选择区域和项目。
  c. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
  d. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
  e. 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”。
  f. 单击“连接”页签，进入VPN连接详情页面。
  g. 在连接日志中，单击“配置连接日志”。
  h. 在弹窗中，开启“启动日志记录”。
  i. 选择目标日志组和日志流，单击确定。

返回“连接”页签，可以看到刚配置的连接日志。

- 查看连接日志
  a. 登录管理控制台。
  b. 在管理控制台左上角单击 图标，选择区域和项目。
  c. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
  d. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
  e. 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”。
  f. 单击“连接”页签，进入VPN连接详情页面。
  g. 在连接日志中，单击“查看详细日志”，进入“云日志服务 LTS”页面。
  h. 在日志组列表，单击日志组左侧图标，查看日志流的详情。
  i. 单击日志流名称，查看日志内容详情，包括时间和日志内容等信息。
  日志内容的上报格式：

```
$p2c_vgw_id $connection_id $client_public_ip $client_private_ip $client_user_name $event_type $event_timestamp
```

表 3-7 上报格式示例说明

参数	说明
p2c_vgw_id	网关ID
connection_id	连接ID
client_public_ip	实际地址
client_private_ip	虚拟地址
client_user_name	用户名称
event_type	上下线事件类型
event_timestamp	时间戳

同时，也可以在“云日志服务 LTS”的日志流详情页面，在搜索框中通过关键字搜索日志。

3.2.20 更新 VPN 连接日志配置

前提条件

用户已经配置VPN连接日志。如何配置连接日志，请参见**配置连接日志**。

操作须知

更新连接日志配置后，原来上报的连接日志将无法在新的连接日志组或日志流中查看，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 单击“连接”页签，进入VPN连接详情页面。

步骤7 在连接日志中，单击“配置连接日志”。

步骤8 在弹窗中，选择需要更新的日志组和日志流。

步骤9 单击确定。

返回“连接”页签，可以看到刚更新的连接日志。

----结束

3.2.21 删除 VPN 连接日志配置

操作须知

删除连接日志配置后，将无法上报连接日志，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

步骤4 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

步骤5 单击“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”。

步骤6 单击“连接”，进入VPN连接详情页面。

步骤7 在连接日志中，单击“配置连接日志”。

步骤8 在弹窗中，选择关闭“启动日志记录”。

步骤9 单击确定。

----结束

3.3 终端入云 VPN 客户端管理

3.3.1 客户端配置须知

约束与限制

- 同一客户端连接多个服务端场景，服务端配置的客户端网段信息不能存在包含或重合关系，否则，VPN客户端连接时可能分配到相同IP地址导致连接失败。
- 同一个客户端设备不能同时与同一个VPN网关建立多条VPN连接，否则只有其中一条VPN连接能通。
- OpenVPN客户端在VPN配置DNS后，会接管或覆盖客户端原始的DNS，导致华为云DNS以外的域名解析失败或无法访问。

高危操作提醒

在配置客户端前，请谨慎操作增删改VPN网关本端子网、VPN连接的对端子网和策略配置，可能会导致网络中断。

操作系统支持列表

表 3-8 操作系统支持列表

操作系统类型	操作系统版本	客户端版本	如何操作
Windows	Windows10及以上	• OpenVPN GUI 2.6及以上版本 • OpenVPN Connect 3.4.4及以上版本	配置Windows客户端
Linux	• Ubuntu 24.10 • Ubuntu 22.04（jammy）	• 24.10系统为OpenVPN 2.6及以上版本 • 22.04系统为OpenVPN 2.5及以下版本	Ubuntu
	• CentOS 7.9 • CentOS 8 • CentOS Stream 9	• 7.9、8系统为OpenVPN 2.4.12版本 • Stream 9系统为OpenVPN 2.5及以上版本	CentOS
	Debian12	OpenVPN 2.5及以上版本	Debian
	Redhat 9.5	OpenVPN 2.5及以上版本	Redhat
	OpenSUSE 15.5	OpenVPN 2.5及以上版本	OpenSUSE
MacOS	-	• Tunnelblick 3.8.8d • OpenVPN Connect 3.4.4.4629	配置Mac客户端
Android	-	OpenVpn Connect APK 3.3.2以上版本	配置Android客户端

操作系统类型	操作系统版本	客户端版本	如何操作
iOS	-	OpenVpn Connect 3.4.0	配置iOS客户端

说明

以上客户端仅3.4.0及以上版本支持IAM和联邦认证。

3.3.2 配置 Windows 客户端

配套版本

Windows版本及相关信息如配套版本所示。

表 3-9 配套版本

客户端类型	OpenVPN版本	如何操作
OpenVPN GUI	2.6及以上版本	OpenVPN GUI
OpenVPN Connect	3.4.4及以上版本	OpenVPN Connect

OpenVPN GUI

步骤1 下载OpenVPN GUI安装包，并根据界面提示进行安装。

不同的Windows操作系统下载的安装包不同，如下是3种操作系统的下载方式。

- Windows 32位操作系统，可以下载Windows 32-bit MSI installer
- Windows 64位操作系统，可以下载Windows 64-bit MSI installer（支持64位的操作系统）
- Windows ARM架构的64位操作系统，可以下载Windows ARM64 MIS installer

步骤2 下载客户端配置文件。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择“终端入云VPN网关”页签，单击目标VPN网关所在行操作列的“下载客户端配置”。

   下载的客户端配置文件为“client_config.zip”。

步骤3 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。

步骤4 以记事本或Notepad++打开“client_config.ovpn”文件。

步骤5 添加客户端证书及私钥。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

步骤6 保存ovpn配置文件。

步骤7 单击开始菜单栏中的“OpenVPN GUI”，启动客户端。

启动后右下角会弹出“OpenVPN GUI 已经运行。右击任务栏图标启动”的提示。

步骤8 右键单击Windows任务栏中的  图标，选择“导入 > 导入配置文件”。

导入ovpn配置文件文件。

导入后右下角会弹出“已成功导入文件”的提示。

步骤9 在“打开”对话框中，选择已添加客户端证书及私钥的配置文件并单击“打开”。

步骤10 右键选中Windows任务栏中的  图标，单击“连接”。

----结束

OpenVPN Connect

步骤1 在OpenVPN官方网站**下载OpenVPN Connect**，根据界面提示进行安装。

步骤2 下载客户端配置文件。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击  图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择“终端入云VPN网关”页签，单击目标VPN网关所在行操作列的“下载客户端配置”。

   下载的客户端配置文件为“client_config.zip”。

步骤3 添加配置信息。

支持以下两种方式添加配置信息。

- **方式1：导入配置文件（已添加客户端证书及私钥）**
  a. 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

     解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。

b. 以记事本或Notepad++打开“client_config.ovpn”文件。

c. 添加客户端证书及私钥。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

d. 保存ovpn配置文件。

e. 打开OpenVPN Connect客户端。

f. 导入ovpn配置文件。

- **方式2：使用原始配置文件（未添加客户端证书及私钥）+USB-Key的组合**

a. 初始化USB-Key。

此处以使用龙脉mToken GM3000管理员工具（v2.2.19.619）制作USB-Key为例。USB-Key初始化成功后，此时需要拔插一下USB设备。

b. 将客户端证书导入USB-Key。

c. 使用USB-Key建立VPN连接。

在OpenVPN Connect中导入USB-Key中未添加客户端CA证书及私钥的配置文件，单击“CONNECT”。

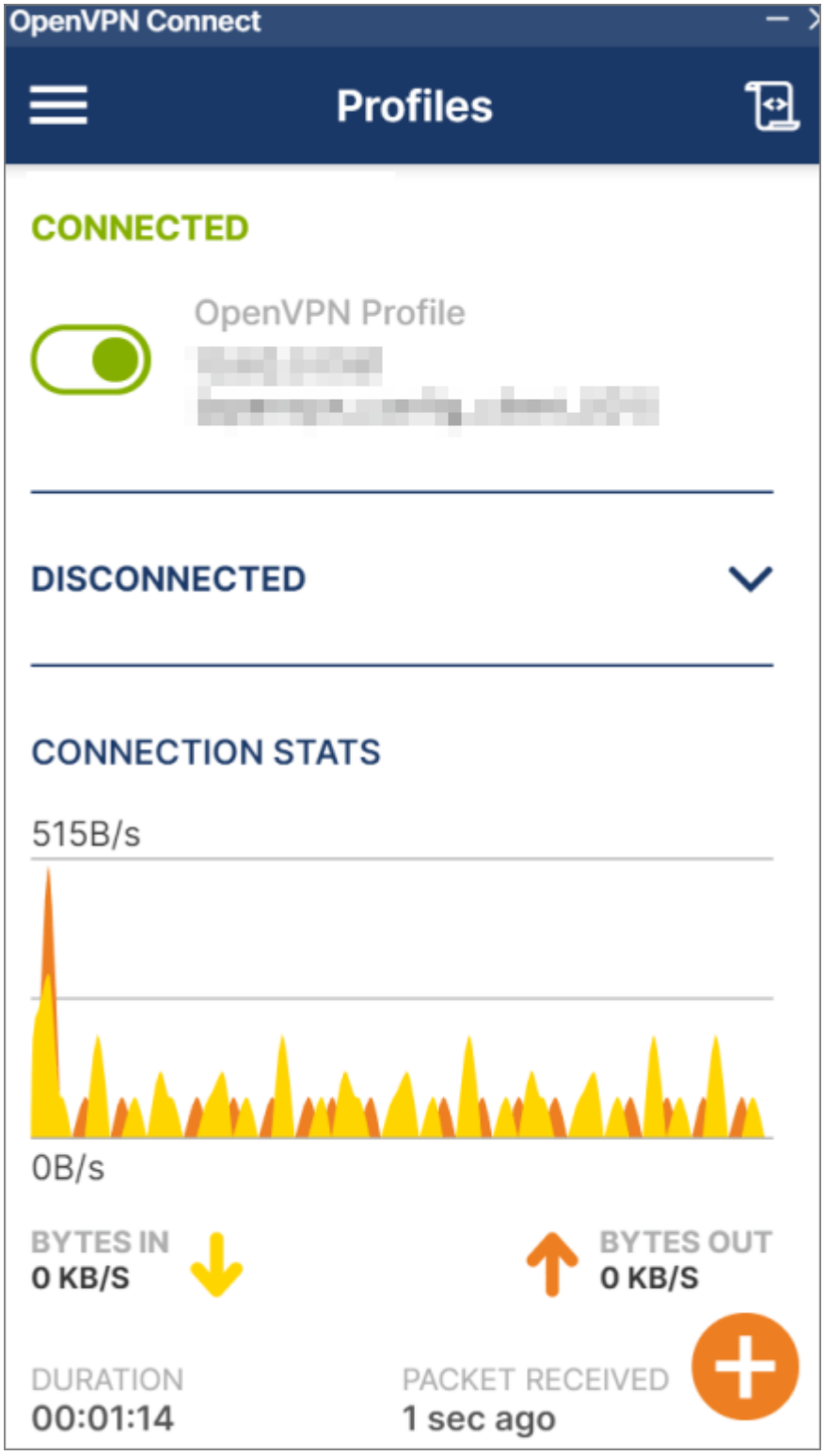
说明

- 建连过程中，USB-Key需要保持插入状态。
- 建连成功后，拔出USB-Key，连接不会中断，需要手动断连；USB-Key拔出后，重新建连将失败。

步骤4 建立VPN连接。

出现类似下图所示界面，代表连接成功。

图 3-3 连接成功



----结束

3.3.3 配置 Linux 客户端

3.3.3.1 Ubuntu

配套版本

Ubuntu版本及相关依赖信息如**配套版本**所示。

表 3-10 配套版本

Ubuntu版本	OpenSSL版本	OpenVPN版本	如何操作
24.10	3.3.1	2.5以上版本	**Ubuntu 24.10**
22.04（jammy）	1.1.1	2.5及以上版本	**Ubuntu 22.04（jammy）**

Ubuntu 24.10

步骤1 以**root**用户登录Ubuntu系统，打开命令行窗口。

步骤2 执行以下命令，备份系统原有的配置文件。

cp -a /etc/apt/sources.list.d/ubuntu.sources /etc/apt/sources.list.d/ubuntu.sources.bak

步骤3 安装apt源。

1. 执行以下命令，配置apt源。

   vim /etc/apt/sources.list.d/ubuntu.sources

2. 在命令框中写入以下内容。

   ```
   Types: deb
   URIs: https://xxx.cn/ubuntu/
   Suites: oracular oracular-updates oracular-backports
   Components: main restricted universe multiverse
   Signed-By: /usr/share/keyrings/ubuntu-archive-keyring.gpg

   Types: deb
   URIs: https://xxx.cn/ubuntu/
   Suites: oracular-security
   Components: main restricted universe multiverse
   Signed-By: /usr/share/keyrings/ubuntu-archive-keyring.gpg
   ```

   说明

   *https://xxx.cn/*请以实际使用源替换。

3. 按“ESC”后，输入**:wq**，按“Enter”。

   保存设置并退出编辑器。

步骤4 执行以下命令，查询当前OpenVPN版本。

openvpn --version

回显如下粗体信息。

```
OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
library versions: OpenSSL 3.3.1 4 Jun 2024, LZO 2.10
```

- 如果系统显示OpenVPN版本，请继续步骤**5**。

- 如果系统不显示OpenVPN版本，请参考以下步骤进行安装。

  a. 执行以下命令，安装OpenVPN。

  apt install -y openvpn

  当系统下载时，会显示一个下载进度条，进度条达到100%即表示安装完成。

  回显如下信息：

```
Installing:
  openvpn

Suggested packages:
  openvpn-dco-dkms  openvpn-systemd-resolved  easy-rsa
......
......
......
No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
```

  b. 再次执行以下命令，查看OpenVPN版本。

  openvpn --version

  回显如下粗体信息：

```
OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
library versions: OpenSSL 3.3.1 4 Jun 2024, LZO 2.10
```

步骤5 在Windows系统，下载客户端配置文件。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择“终端入云VPN网关”页签，单击目标VPN网关所在行操作列的“下载客户端配置”。

   下载的客户端配置文件为“client_config.zip”。

步骤6 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。

步骤7 以记事本或Notepad++打开“client_config.conf”文件。

步骤8 添加客户端证书及私钥。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```


步骤9 保存conf配置文件。

步骤10 将conf配置文件用Xftp文件传输工具上传到Ubuntu系统。本示例中上传至“/opt/”目录下。

步骤11 在Ubuntu系统，执行以下命令，进入客户端配置文件所在目录。

cd /opt/

步骤12 执行以下命令，启动OpenVPN客户端并连接VPN网关。

openvpn --config /opt/openvpn_config_user-01.conf

回显如下粗体信息，表示OpenVPN连接建立成功。

```
2025-02-27 19:22:41 Note: Kernel support for conf-dco missing, disabling data channel offload.
2025-02-27 19:22:41 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-02-27 19:22:41 library versions: OpenSSL 3.3.1 4 Jun 2024, LZO 2.10
......
......
......
2025-02-27 19:22:42 Initialization Sequence Completed
......
......
```

步骤13 执行以下命令，验证连通性。

ping XX.XX.XX.XX

说明

XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

----结束

Ubuntu 22.04（jammy）

步骤1 以**root**用户登录Ubuntu系统，打开命令行窗口。

步骤2 执行以下命令，安装OpenVPN客户端。

yum install -y openvpn

步骤3 在Windows系统，下载客户端配置文件。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择“终端入云VPN网关”页签，单击目标VPN网关所在行操作列的“下载客户端配置”。

下载的客户端配置文件为“client_config.zip”。

6. 解压缩“client_config.zip”至指定目录，如“D:\”目录下。
   解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。
7. 以记事本或Notepad++打开“client_config.conf”文件。
8. 添加客户端证书及私钥。
   在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

9. （可选）注释“disable-dco”。仅OpenVPN使用**2.5及以下版本**时涉及。
   a. 按**Ctrl+F**定位“disable-dco”参数的所在位置。
   b. 在“disable-dco”所在行前输入**#**注释该行信息。

```
.....
.....
# disable-dco
.....
.....
```

10. 保存conf配置文件。

步骤4 将conf配置文件用Xftp文件传输工具上传到Ubuntu。本示例中上传至“/etc/openvpn/conf/”目录下。

步骤5 在Ubuntu系统，执行以下命令，进入客户端配置文件所在目录。

cd /etc/openvpn/conf/

步骤6 执行以下命令，启动OpenVPN客户端并连接VPN网关。

openvpn --config /etc/openvpn/conf/config.conf --daemon

说明

在Linux系统里，启动OpenVPN后，建议不要修改操作系统的DNS配置，否则在下次启动OpenVPN时，OS的DNS配置会被OpenVPN客户端里的DNS配置覆盖。

----结束

3.3.3.2 CentOS

配套版本

CentOS版本及相关依赖信息如**配套版本**所示。

表 3-11 配套版本

CentOS版本	OpenSSL版本	OpenVPN版本
7.9	1.1.1	2.4.12
8	1.1.1	2.4.12
Stream9	3.2.2	2.5及以上版本

操作步骤

步骤1 以**root**用户登录CentOS系统，打开命令行窗口。

步骤2 执行以下命令，备份系统原有的配置文件。

cp -a /etc/yum.repos.d/epel.repo /etc/yum.repos.d/epel.repo.backup

步骤3 安装epel源。

- CentOS 7.9
  执行以下命令，安装epel源。
  yum install -y epel-release
  回显如下信息，表示epel源安装成功。

```
Last metadata expiration check: 0:00:14 ago on Wed 05 Mar 2025 05:53:17 PM CST.
.....
.....
.....
Installed:
  epel-release-8-11.el8.noarch

Complete!
```

- CentOS 8、Stream9
  a. 执行以下命令，配置epel源。
  vim /etc/yum.repos.d/epel.repo
  b. 在命令框中写入以下内容。

```
[epel]
name=epel
baseurl=https://xxx.cn/epel/8/Everything/x86_64/
gpgcheck=0
gpgkey=https://xxx.cn/epel/RPM-GPG-KEY-EPEL-8
```

  说明
  - **8**表示CentOS版本，请根据实际版本修改。
  - ***https://xxx.cn/***请以实际使用源替换。

  c. 按“ESC”后，输入**:wq**，按“Enter”。
  保存设置并退出编辑器。

步骤4 执行以下命令，查询当前OpenSSL版本。

openssl version

回显如下信息：


```
OpenSSL 1.1.1k
```

- 如果系统显示的是OpenSSL1.1.1k及以上版本，请继续步骤**5**。
- 如果系统显示的是OpenSSL1.1.1k以下版本，请参考以下步骤安装OpenSSL。
  a. 执行以下命令，安装OpenSSL 1.1.1k。
     yum install -y openssl11 openssl11-devel
     回显如下信息，表示OpenSSL 1.1.1k安装成功。

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
......
......
......
Is this ok [y/d/N]: y     # 输入y以继续
......
......
......
Installed:
  openssl11.x86_64 1:1.1.1k-7.el7

Complete!
```

  b. 再次执行以下命令，查询OpenSSL版本。
     openssl11 version
     回显如下信息：

```
OpenSSL 1.1.1k
```

步骤5 执行以下命令，查询当前OpenVPN版本。

openvpn --version

回显如下信息：

```
OpenVPN 2.4.12 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO]
[AEAD] built on Nov 10 2023
library versions: OpenSSL 1.1.1k FIPS 25 Mar 2021, LZO 2.08
```

- 如果系统显示OpenVPN版本，请继续步骤**6**。
- 如果系统不显示OpenVPN版本，请参考以下步骤安装OpenVPN。
  安装OpenVPN。不同CentOS版本的安装命令不同，请根据实际系统执行。
  - CentOS 7.9

    说明

    CentOS 7.9仅支持安装OpenVPN 2.4.12版本，不支持其他版本。

    i. 在Windows系统，下载OpenVPN客户端安装包（**openvpn-2.4.12-2.el8.rpm**）。
    ii. 将下载的rpm安装包用Xftp文件传输工具上传到CentOS的目录下。本示例中上传至“/opt/”目录下。
    iii. 在CentOS系统，执行以下命令，进入安装包所在目录。
         cd /opt/
    iv. 执行以下命令，安装OpenVPN。
        yum install ./openvpn-2.4.12-2.el8.x86_64.rpm
        回显如下粗体信息，表示OpenVPN安装成功。

```
Loaded plugins: fastestmirror
Examining openvpn-2.4.12-2.el8.x86_64.rpm: openvpn-2.4.12-2.el8.x86_64
Marking openvpn-2.4.12-2.el8.x86_64.rpm to be installed
```



```
.....
.....
.....
Is this ok [y/d/N]: y          # 输入y以继续
.....
.....
.....
Installed:
  openvpn.x86_64 0:2.4.12-2.el8

Complete!
```

v. 再次执行以下命令，查询OpenVPN版本。

openvpn --version

回显如下粗体信息：

```
OpenVPN 2.4.12 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
[PKCS11] [MH/PKTINFO] [AEAD] built on Nov 10 2023
library versions: OpenSSL 1.1.1k FIPS 25 Mar 2021, LZO 2.08
```

- CentOS 8、CentOS Stream9

i. 在CentOS系统，执行以下命令，安装OpenVPN。

yum install openvpn

回显如下粗体信息，表示OpenVPN安装成功。

```
CentOS-8 - Base                              28 kB/s | 3.9 kB     00:00
.....
.....
.....
Is this ok [y/N]: y              # 输入y以继续
.....
.....
.....
Installed:
  openvpn-2.4.12-2.el8.x86_64            pkcs11-helper-1.22-7.el8.x86_64

Complete!
```

ii. 再次执行以下命令，查询OpenVPN版本。

openvpn --version

回显如下粗体信息：

```
OpenVPN 2.4.12 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
[PKCS11] [MH/PKTINFO] [AEAD] built on Nov 10 2023
library versions: OpenSSL 1.1.1k FIPS 25 Mar 2021, LZO 2.08
```

步骤6 在Windows系统，下载客户端配置文件。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择“终端入云VPN网关”页签，单击目标VPN网关所在行操作列的“下载客户端配置”。

   下载的客户端配置文件为“client_config.zip”。
6. 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

   解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。
7. 以记事本或Notepad++打开“client_config.conf”文件。
8. 添加客户端证书及私钥。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

9. （可选）注释“data-ciphers”和“disable-dco”。

   说明

   “data-ciphers”参数仅OpenVPN使用2.4.12版本时需要注释。

   “disable-dco”参数仅OpenVPN使用2.5及以下版本时需要注释。

   a. 按**Ctrl+F**定位“data-ciphers”和“disable-dco”参数的所在位置。

   b. 在参数所在行前输入**#**注释该行信息。

   ```
   ......
   ......
   # data-ciphers AES-XXX-GCM      # 仅CentOS 7.9和CentOS 8需要注释
   ......
   ......
   # disable-dco                   # CentOS 7.9、CentOS 8和CentOS Stream9都需要注释
   ......
   ......
   ```

10. 保存conf配置文件。

步骤7 将conf配置文件用Xftp文件传输工具上传到CentOS系统。本示例中上传至“/opt/”目录下。

步骤8 在CentOS系统，执行以下命令，进入客户端配置文件所在目录。

cd /opt/

步骤9 执行以下命令，启动OpenVPN客户端并连接VPN网关。

openvpn --config /opt/openvpn_config_user-01.conf

回显如下粗体信息，表示OpenVPN连接建立成功。

```
Tue Feb 25 19:24:04 2025 OpenVPN 2.4.12 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Nov 10 2023
......
......
......
Tue Feb 25 19:24:06 2025 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Tue Feb 25 19:24:06 2025 Initialization Sequence Completed
```

步骤10 执行以下命令，验证连通性。

ping XX.XX.XX.XX

说明

XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
```



```
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

----结束

3.3.3.3 Debian

配套版本

Debian版本及相关依赖信息如**配套版本**所示。

表 3-12 配套版本

Debian版本	OpenSSL版本	OpenVPN版本
12.0.0	1.1.1	2.5及以上版本

高危操作提醒

在配置客户端前，请谨慎操作增删改VPN网关本端子网、VPN连接的对端子网和策略配置，可能会导致网络中断。

操作步骤

步骤1 以**root**用户登录Debian系统，打开命令行窗口。

步骤2 执行以下命令，备份系统原有的配置文件。

cp -a /etc/apt/sources.list /etc/apt/sources.list.bak

步骤3 安装apt源。

1. 执行以下命令，配置apt源。

   vi /etc/apt/sources.list

2. 在命令框中写入以下内容。

   ```
   deb https://xxx.cn/debian/ bullseye contrib main

   deb-src https://xxx.cn/debian/ bullseye contrib main

   #软件更新源

   deb https://xxx.cn/debian-security/ bullseye-security main contrib

   deb-src https://xxx.cn/debian-security/ bullseye-security main contrib

   #安全更新源

   deb https://xxx.cn/debian/ bullseye-updates main contrib

   deb-src https://xxx.cn/debian/ bullseye-updates main contrib
   ```

   说明

   *https://xxx.cn/*请以实际使用源替换。

3. 按“ESC”后，输入**:wq**，按“Enter”。

保存设置并退出编辑器。

步骤4 执行以下命令，查看版本信息。

openvpn --version

回显如下信息：

```
OpenVPN 2.5.1 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
library versions: OpenSSL 1.1.1w  11 Sep 2023, LZO 2.10
```

- 如果系统显示OpenVPN版本，请继续步骤5。
- 如果系统不显示OpenVPN版本，请参考以下步骤安装OpenVPN。
  a. 执行以下命令，安装OpenVPN。

  apt install -y openvpn

  当系统下载时，下方会显示一个下载进度条，进度条达到100%即表示安装完成。

  回显如下信息：

  ```
  Reading package lists... Done
  Building dependency tree... Done
  Reading state information... Done
  ......
  ......
  ......
  Unpacking openvpn (2.5.1-3) ...
  Setting up openvpn (2.5.1-3) ...
  Processing triggers for man-db (2.11.2-2) ...
  ```

  b. 再次执行以下命令，查看版本信息。

  openvpn --version

  回显如下信息：

  ```
  OpenVPN 2.5.1 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
  library versions: OpenSSL 1.1.1w  11 Sep 2023, LZO 2.10
  ```

步骤5 在Windows系统，下载客户端配置文件。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择“终端入云VPN网关”页签，单击目标VPN网关所在行操作列的“下载客户端配置”。

   下载的客户端配置文件为“client_config.zip”。

步骤6 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。

步骤7 以记事本或Notepad++打开“client_config.conf”文件。

步骤8 添加客户端证书及私钥。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
```



```
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

步骤9 （可选）注释“disable-dco”。仅OpenVPN使用**2.5及以下版本**时涉及。

1. 按**Ctrl+F**定位“disable-dco”参数的所在位置。
2. 在“disable-dco”所在行前输入**#**注释该行信息。

```
.....
.....
# disable-dco
.....
.....
```

步骤10 保存conf配置文件。

步骤11 将conf配置文件用Xftp文件传输工具上传到Debian系统。本示例中上传至“/opt/”目录下。

步骤12 执行以下命令，进入安装包所在目录。

cd /opt/

步骤13 执行以下命令，启动OpenVPN客户端并连接VPN网关。

openvpn --config /opt/openvpn_config_user-01.conf

回显如下粗体信息，表示OpenVPN连接建立成功。

```
2025-02-28 11:34:35 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2025-02-28 11:34:35 library versions: OpenSSL 1.1.1w  11 Sep 2023, LZO 2.10
...
...
...
2025-02-28 11:34:37 Initialization Sequence Completed
```

步骤14 执行以下命令，验证连通性。

ping XX.XX.XX.XX

说明

XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

----结束

3.3.3.4 RedHat Linux

配套版本

RedHat Linux版本及相关依赖信息如**配套版本**所示。

表 3-13 配套版本

RedHat Linux版本	OpenSSL版本	OpenVPN版本
9.5	1.1.1及以上	2.5及以上版本

操作步骤

步骤1 在Windows系统下载lib64pkcs11-helper1。

步骤2 将下载的rpm安装包用Xftp文件传输工具上传到Redhat的目录下。本示例中上传至“/opt/”目录下。

步骤3 以**root**用户登录RedHat Linux系统，打开命令行窗口。

步骤4 执行以下命令，进入安装包所在目录。

cd /opt/

步骤5 执行以下命令，安装lib64pkcs11-helper1。

yum install lib64pkcs11-helper1-1.30.0-1-omv2390.x86_64.rpm

回显如下信息，表示lib64pkcs11-helper1安装成功。

```
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use "rhc" or "subscription-manager" to register.
...
...
...
Installed:
  lib64pkcs11-helper1-1.30.0-1.x86_64

Complete!
```

步骤6 执行以下命令，查看OpenVPN版本。

openvpn --version

回显如下信息：

```
OpenVPN 2.5.11 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Jul 18 2024
library versions: OpenSSL 3.2.2 4 Jun 2024, LZO 2.10
```

- 如果系统显示OpenVPN版本，请继续步骤4。
- 如果系统不显示OpenVPN版本，请参考以下步骤安装OpenVPN。
  a. 在Windows系统下载OpenVPN。
  b. 将下载的rpm安装包用Xftp文件传输工具上传到Redhat的目录下。本示例中上传至“/opt/”目录下。
  c. 执行以下命令，安装OpenVPN。

     yum install openvpn-2.5.11-1.el9.x86_64.rpm

     回显如下粗体信息，表示OpenVPN安装成功。

     ```
     Updating Subscription Management repositories.
     Unable to read consumer identity
     ...
     ...
     ```



```
...
Is this ok [y/N]: y                    # 输入y以继续
...
...
...
Installed:
  openvpn-2.5.11-1.el9.x86_64

Complete!
```

d. 再次执行以下命令，查看OpenVPN版本。

openvpn --version

回显如下粗体信息：

```
OpenVPN 2.5.11 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11]
[MH/PKTINFO] [AEAD] built on Jul 18 2024
library versions: OpenSSL 3.2.2 4 Jun 2024, LZO 2.10
```

步骤7 在Windows系统，下载客户端配置文件。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择“终端入云VPN网关”页签，单击目标VPN网关所在行操作列的“下载客户端配置”。

   下载的客户端配置文件为“client_config.zip”。

步骤8 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。

步骤9 以记事本或Notepad++打开“client_config.conf”。

步骤10 添加客户端证书及私钥。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

步骤11 （可选）注释“disable-dco”。仅OpenVPN使用**2.5及以下版本**时涉及。

1. 按**Ctrl+F**定位“disable-dco”参数的所在位置。
2. 在“disable-dco”所在行前输入**#**注释该行信息。

```
.....
.....
# disable-dco
.....
.....
```

步骤12 保存conf配置文件。

步骤13 将conf配置文件用Xftp文件传输工具上传到Redhat系统。本示例中上传至“/opt/”目录下。

步骤14 执行以下命令，进入客户端配置文件所在目录。

cd /opt/

步骤15 执行以下命令，启动OpenVPN客户端并连接VPN网关。

openvpn --config /opt/openvpn_config_user-01.conf

回显如下粗体信息，表示OpenVPN连接建立成功。

```
2025-02-27 22:18:30 OpenVPN 2.5.11 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
[PKCS11] [MH/PKTINFO] [AEAD] built on Jul 18 2024
2025-02-27 22:18:30 library versions: OpenSSL 3.2.2 4 Jun 2024, LZO 2.10
...
...
...
2025-02-27 22:18:32 Initialization Sequence Completed
```

步骤16 执行以下命令，验证连通性。

ping XX.XX.XX.XX

说明

XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

----结束

3.3.3.5 OpenSUSE

配套版本

OpenSUSE版本及相关依赖信息如**配套版本**所示。

表 3-14 配套版本

OpenSUSE版本	OpenSSL版本	OpenVPN版本
15.5	1.1.1	2.5及以上版本

操作步骤

步骤1 以**root**用户登录CentOS系统，打开命令行窗口。

步骤2 配置zypper源。

1. 执行以下命令，备份系统原有的配置文件。

   mkdir /etc/zypp/repos.d/repo_bakmv /etc/zypp/repos.d/*.repo /etc

   /zypp/repos.d/repo_bak/mv /etc/zypp/repos.d/*.repo /etc/zypp/repos.d/repo_bak/

2. 配置镜像源。

   说明

   客户端版本不同，镜像源配置也不同。具体配置请参考配置zypper源相关文档。

步骤3 执行以下命令，查看版本信息。

openvpn --version

回显如下信息：

```
OpenVPN 2.5.6 x86_64-suse-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Mar 16 2022
library versions: OpenSSL 1.1.1l  24 Aug 2021 SUSE release 150500.15.4, LZO 2.10
```

- 如果系统显示OpenVPN版本，请继续步骤4。
- 如果系统不显示OpenVPN版本，请参考以下步骤安装OpenVPN。

  a. 执行以下命令，安装OpenVPN。

  zypper install openvpn

  回显如下信息，表示OpenVPN安装成功。

  ```
  Loading repository data...
  ......
  ......
  ......
  Continue? [y/n/v/...? shows all options] (y): y            # v输入y以继续
  ......
  ......
  ......
  (1/1) Installing: openvpn-2.5.6-150400.3.6.1.x86_64 .....[done]
  ```

  b. 再次执行以下命令，查看版本信息。

  openvpn --version

  回显如下粗体信息：

  ```
  OpenVPN 2.5.6 x86_64-suse-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Mar 16 2022
  library versions: OpenSSL 1.1.1l  24 Aug 2021 SUSE release 150500.15.4, LZO 2.10
  ```

步骤4 在Windows系统，下载客户端配置文件。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择“终端入云VPN网关”页签，单击目标VPN网关所在行操作列的“下载客户端配置”。

   下载的客户端配置文件为“client_config.zip”。

步骤5 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。

步骤6 以记事本或Notepad++打开“client_config.conf”文件。

步骤7 添加客户端证书及私钥。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
```



```
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

步骤8 （可选）注释“disable-dco”。仅OpenVPN使用**2.5及以下版本**时涉及。

1. 按**Ctrl+F**定位“disable-dco”参数的所在位置。
2. 在“disable-dco”所在行前输入**#**注释该行信息。

```
.....
.....
# disable-dco
.....
.....
```

步骤9 保存conf配置文件。

步骤10 将conf配置文件用Xftp文件传输工具上传到OpenSUSE系统，本示例中上传至“/opt/”目录下。

步骤11 在OpenSUSE系统，执行以下命令，进入客户端配置文件所在目录。

cd /opt/

步骤12 执行以下命令，启动OpenVPN客户端并连接VPN网关。

openvpn --config /opt/openvpn_config_user-01.conf

回显如下粗体信息，表示OpenVPN连接建立成功。

```
2025-02-27 14:09:26 OpenVPN 2.5.6 x86_64-suse-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
[PKCS11] [MH/PKTINFO] [AEAD] built on Mar 16 2022
2025-02-27 14:09:26 library versions: OpenSSL 1.1.1l  24 Aug 2021 SUSE release 150500.15.4, LZO 2.10
...
...
...
2025-02-27 14:09:28 Initialization Sequence Completed
```

步骤13 执行以下命令，验证连通性。

ping XX.XX.XX.XX

说明

XX.XX.XX.XX为想要连接的ECS私网IP，请根据实际替换。

回显如下信息，表示网络已通。

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

----结束

3.3.4 配置 MacOS 客户端

客户端版本

MacOS支持的客户端及相关版本信息如**客户端版本**所示。

表 3-15 客户端版本

客户端	客户端版本	如何操作
OpenVPN Connect	3.4.4.4629	**OpenVPN Connect**
Tunnelblick	3.8.8d	**Tunnelblick**

OpenVPN Connect

步骤1 在OpenVPN官方网站**下载OpenVPN Connect**，根据硬件规格选择对应安装程序。

步骤2 根据界面提示，完成软件安装。

步骤3 下载客户端配置文件。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择“终端入云VPN网关”页签，单击目标VPN网关所在行操作列的“下载客户端配置”。

   下载的客户端配置文件为“client_config.zip”。

步骤4 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。

步骤5 以文本编辑方式打开“client_config.ovpn”文件。

步骤6 添加客户端证书及私钥。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

步骤7 保存ovpn配置文件。

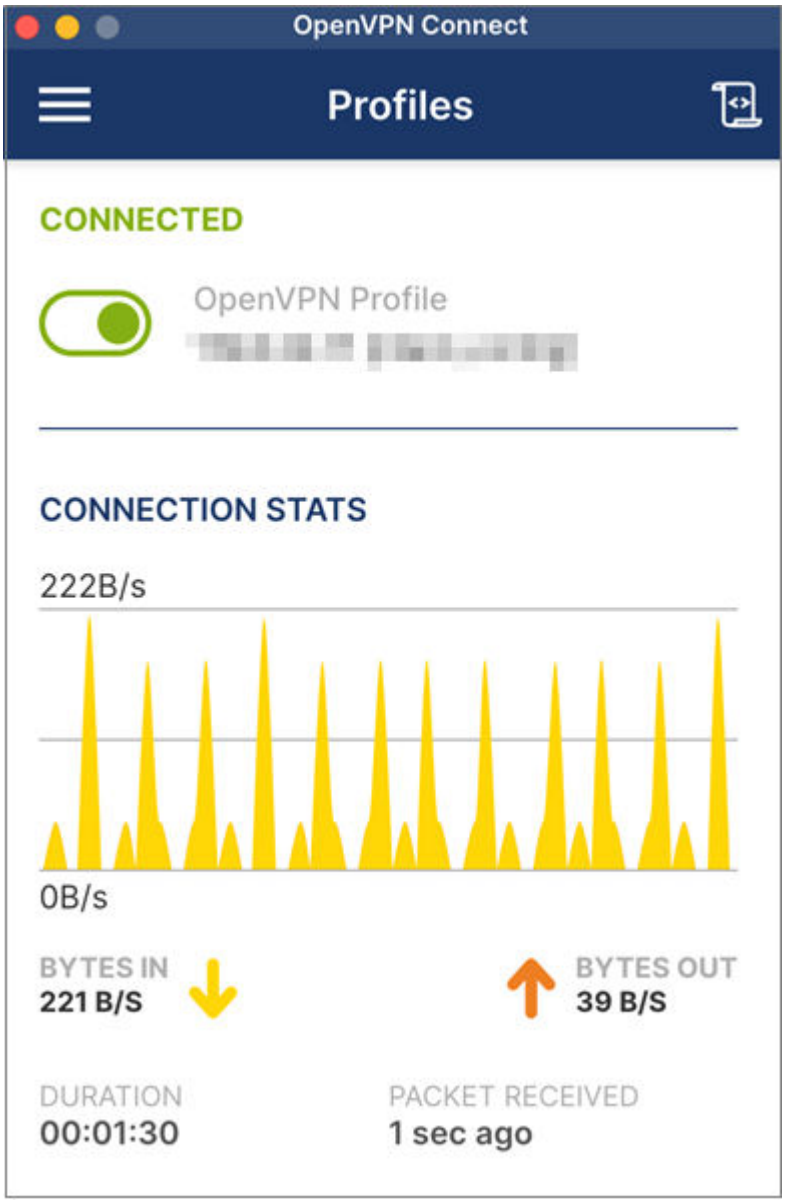
步骤8 打开OpenVPN Connect客户端。

步骤9 导入ovpn配置文件，填写配置信息。

步骤10 建立VPN连接。

出现类似下图所示界面，代表连接成功。

图 3-4 连接成功



----结束

Tunnelblick

步骤1 前往官方网站下载Tunnelblick。

您可以根据实际需要下载适用的版本，推荐使用正式版本。下载软件时推荐下载DMG格式的软件。

步骤2 根据界面提示，安装Tunnelblick。

步骤3 下载客户端配置文件。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择“终端入云VPN网关”页签，单击目标VPN网关所在行操作列的“下载客户端配置”。

   下载的客户端配置文件为“client_config.zip”。

步骤4 解压缩“client_config.zip”至指定目录，如“D:\”目录下。

解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。

步骤5 以文本编辑方式打开“client_config.ovpn”文件。

步骤6 添加客户端证书及私钥。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

步骤7 注释“disable-dco”。

1. 按**Command+F**定位“disable-dco”参数的所在位置。
2. 在“disable-dco”所在行前输入**#**注释该行信息。

```
.....
.....
# disable-dco
.....
.....
```

步骤8 保存ovpn配置文件。

步骤9 打开Tunnelblick客户端。

步骤10 导入ovpn配置文件。

步骤11 建立VPN连接。

----结束

3.3.5 配置 Android 客户端

操作步骤

步骤1 下载**OpenVPN客户端（Android版本）**并安装。

步骤2 下载客户端配置文件。

- 方式1：通过PC下载客户端配置文件。
- 方式2：通过手机下载客户端配置文件。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 选择“终端入云VPN网关”页签，单击目标VPN网关所在行操作列的“下载客户端配置”。

   下载的客户端配置文件为“client_config.zip”。

   说明

   通过PC下载客户端配置文件，需要将已下载的配置文件上传到Android系统中。

步骤3 在PC上，解压缩“client_config.zip”至指定目录，如“D:\”目录下。

解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。

步骤4 以记事本或Notepad++打开“client_config.ovpn”文件。

步骤5 添加客户端证书及私钥。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

步骤6 保存ovpn配置文件。

说明

如果在Android手机上操作，需要将PC上已配置的ovpn配置文件上传到Android系统中。

步骤7 打开OpenVPN客户端。

- 方式1：通过PC打开客户端。
- 方式2：通过手机打开客户端。

步骤8 导入ovpn配置文件。

步骤9 建立VPN连接。

此时APP界面将弹出连接请求提示，请单击确定。

出现类似下图所示界面，代表连接成功。

图 3-5 连接成功

----结束

3.3.6 配置 iOS 客户端

操作步骤

步骤1 在App Store搜索“OpenVPN Connect”，下载并安装。

步骤2 下载客户端配置文件。

- **方式1：通过PC下载客户端配置文件。**
- **方式2：通过手机下载客户端配置文件。**

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。

5. 选择“终端入云VPN网关”页签，单击目标VPN网关所在行操作列的“下载客户端配置”。

   下载的客户端配置文件为“client_config.zip”。

   说明

   通过PC下载客户端配置文件，需要将已下载的配置文件上传到Android系统中。

步骤3 在PC上，解压缩“client_config.zip”至指定目录，如“D:\”目录下。

解压缩后，可以得到“client_config.ovpn”和“client_config.conf”两个文件。

步骤4 以记事本或Notepad++打开“client_config.ovpn”文件。

步骤5 添加客户端证书及私钥。

在<cert></cert>和<key></key>标记对内分别填写客户端证书、客户端证书私钥。

```
<cert>
-----BEGIN CERTIFICATE-----
此处添加客户端证书
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
此处添加客户端私钥
-----END PRIVATE KEY-----
</key>
```

步骤6 保存ovpn配置文件。

说明

如果在iOS手机上操作，需要将PC上已配置的ovpn配置文件上传到iOS系统中。

步骤7 打开OpenVPN Connect客户端。

- 方式1：通过PC打开客户端。
- 方式2：通过手机打开客户端。

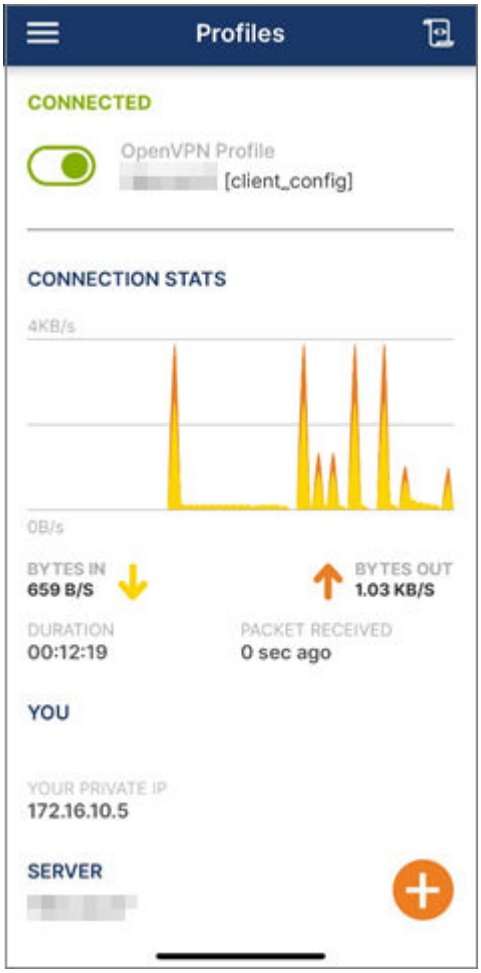
步骤8 导入ovpn配置文件。

按照界面提示添加客户端配置。

步骤9 建立VPN连接。

出现类似下图所示界面，代表连接成功。

图 3-6 连接成功



----结束

3.4 终端入云 VPN 费用管理

3.4.1 包年/包月 VPN 连接数升配/降配

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 单击“终端入云VPN网关”进入终端入云VPN网关页面。
6. 在VPN网关所在行，选择“更多 > 修改VPN连接数”。
7. 在“修改VPN连接数”界面，选择“补差价升配/续费降配”,单击“是”。
8. 选择目标连接数，单击“下一步”。

9. 确认修改详情后，单击“去支付”，完成升降配操作。

说明

- 包年/包月的计费模式下，支持的最大连接数为500。
- 补差价升配可以增加当前网关连接数，升配后新连接数大小在已有的时间周期内立即生效。
- 续费降配支持在新的续费周期内减少网关连接数，您需要选择续费时长并根据修改后的连接数大小支付相应费用；续费成功后新的连接数规格将会在新的计费周期生效。

4 监控

4.1 监控虚拟专用网络

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

相关链接：

更多关于监控的信息，请参见**《云监控用户指南》**。

4.2 支持的监控指标（站点入云 VPN 企业版）

功能说明

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

说明

云监控服务最大支持4个层级维度，维度编号从0开始，编号3为最深层级。例如监控指标中的维度信息为“evpn_connection_id,evpn_sa_id”时，表示对应的监控指标的维度存在层级关系，且“evpn_connection_id”为0层，“evpn_sa_id”为1层。

命名空间

SYS.VPN

监控指标

表 4-1 企业版 VPN 网关支持的监控指标

指标ID	指标名称	指标含义	取值范围	单位	进制	维度	监控周期（原始指标）
gateway_send_pkt_rate	出云包速率	该指标用于统计测量对象平均每秒出云的数据包数量。	≥ 0	pps	不涉及	evpn_gateway_id	1分钟
gateway_recv_pkt_rate	入云包速率	该指标用于统计测量对象平均每秒入云的数据包数量。	≥ 0	pps	不涉及	evpn_gateway_id	1分钟
gateway_send_rate	出云带宽	该指标用于统计测量对象平均每秒出云流量。	0-1	bps	1024(IEC)	evpn_gateway_id	1分钟
gateway_recv_rate	入云带宽	该指标用于统计测量对象平均每秒入云流量。	0-1	bps	1024(IEC)	evpn_gateway_id	1分钟
gateway_send_rate_usage	出云带宽使用率	该指标用于统计测量对象出云带宽使用率。	0-100	percentage(%)	不涉及	evpn_gateway_id	1分钟
gateway_recv_rate_usage	入云带宽使用率	该指标用于统计测量对象入云带宽使用率。	0-100	percentage(%)	不涉及	evpn_gateway_id	1分钟
gateway_connection_num	连接数	该指标用于统计测量对象关联VPN连接数。	≥ 0	count	不涉及	evpn_gateway_id	1分钟

表 4-2 企业版 VPN 连接支持的监控指标

指标ID	指标名称	指标含义	取值范围	单位	进制	维度	监控周期（原始指标）
tunnel_average_latency	隧道往返平均时延	VPN网关与对端网关之间隧道的往返平均时延。	0~5000	ms	不涉及	evpn_connection_id	10s
tunnel_max_latency	隧道往返最大时延	VPN网关与对端网关之间隧道的往返最大时延。	0~5000	ms	不涉及	evpn_connection_id	10s
tunnel_packet_loss_rate	隧道丢包率	VPN网关与对端网关之间隧道的丢包率。	0~100	percentage(%)	不涉及	evpn_connection_id	10s
link_average_latency	链路往返平均时延	VPN网关与对端网关之间链路的往返平均时延。	0~5000	s	不涉及	evpn_connection_id	10s
link_max_latency	链路往返最大时延	VPN网关与对端网关之间链路的往返最大时延。	0~5000	ms	不涉及	evpn_connection_id	10s
link_packet_loss_rate	链路丢包率	VPN网关与对端网关之间链路的丢包率。	0~100	percentage(%)	不涉及	evpn_connection_id	10s
connection_status	VPN连接状态	展示VPN连接的通断状态。 ● 0：未连接状态。 ● 1：连接状态。 ● 2：未知状态。	0，1，2	不涉及	不涉及	evpn_connection_id	1分钟
bgp_peer_status	BGP邻居状态指标	展示BGP邻居的建连状态。 ● 0：未连接状态。 ● 1：连接状态。 ● 2：未知状态。	0，1，2	不涉及	不涉及	evpn_connection_id	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	维度	监控周期（原始指标）
recv_pkt_rate（已废弃，不推荐使用）	接收包速率	平均每秒接收的数据包数量。	≥ 0	pps	不涉及	evpn_connection_id	1分钟
send_pkt_rate（已废弃，不推荐使用）	发送包速率	平均每秒发送的数据包数量。	≥ 0	pps	不涉及	evpn_connection_id	1分钟
recv_rate（已废弃，不推荐使用）	接收速率	平均每秒接收流量。	0~1	bps	1024(IEC)	evpn_connection_id	1分钟
send_rate（已废弃，不推荐使用）	发送速率	平均每秒发送流量。	0~1	bps	1024(IEC)	evpn_connection_id	1分钟
sa_send_pkt_rate	SA发送包速率	平均每秒发送的数据包数量。	≥ 0	pps	不涉及	evpn_connection_id,evpn_sa_id	1分钟
sa_recv_pkt_rate	SA接收包速率	平均每秒接收的数据包数量。	≥ 0	pps	不涉及	evpn_connection_id,evpn_sa_id	1分钟
sa_recv_rate	SA接收速率	平均每秒接收流量。	0~1	bps	1024(IEC)	evpn_connection_id,evpn_sa_id	1分钟
sa_send_rate	SA发送速率	平均每秒发送流量。	0~1	bps	1024(IEC)	evpn_connection_id,evpn_sa_id	1分钟

说明

以下指标需要将VPN网关升级至最新版本，以实现10s的监控周期，实际监控周期请以管理控制台显示为准。

隧道往返平均时延、隧道往返最大时延、隧道丢包率、链路往返平均时延、链路往返最大时延、链路丢包率。

对于有多层测量维度的测量对象，使用接口查询监控指标时，需要代入具体指标的维度层级关系。

例如，需要查询虚拟专用网络中某个VPN连接的SA发送包速率（sa_send_pkt_rate），该指标的维度信息为“evpn_connection_id,evpn_sa_id”，表示evpn_connection_id为0层，evpn_sa_id为1层。

- 通过API查询单个SA指标时，维度信息代入样例如下：

```
dim.0=evpn_connection_id,2C2291dde7-193f-4fb8-9606-40c31e147422&dim.1=evpn_sa_id,2C7965df5f-2e83-4d87-8681-78f69e6c4185
```

其中，2C2291dde7-193f-4fb8-9606-40c31e147422和2C7965df5f-2e83-4d87-8681-78f69e6c4185分别为evpn_connection_id和evpn_sa_id的维度值，具体获取方法请参见“**维度**”表格中的获取指导。

- 通过API批量查询SA指标时，维度信息代入样例如下：

```
"dimensions": [
            {
               "name": "evpn_connection_id",
               "value": "2C2291dde7-193f-4fb8-9606-40c31e147422"
            },
            {
               "name": "evpn_sa_id",
               "value": "2C7965df5f-2e83-4d87-8681-78f69e6c4185"
            },
            {
               "name": "evpn_sa_id",
               "value": "506afac2-1f95-4dad-a73a-a726ad125723"
            }
         ]
```

其中，2C2291dde7-193f-4fb8-9606-40c31e147422、2C7965df5f-2e83-4d87-8681-78f69e6c4185、506afac2-1f95-4dad-a73a-a726ad125723分别为evpn_connection_id和evpn_sa_id的维度值，具体获取方法请参见“**维度**”表格中的获取指导。

维度

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

4.3 支持的监控指标（站点入云 VPN 经典版）

功能说明

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

命名空间

SYS.VPC

监控指标

表 4-3 经典版 VPN 带宽支持的监控指标

指标ID	指标名称	指标含义	取值范围	单位	进制	维度	监控周期（原始指标）
upstream_bandwidth	出网带宽	该指标用于统计测试对象出云平台的网络速度（原指标为上行带宽）。	≥ 0	bit/s	1000(SI)	• bandwidth_id • publicip_id	1分钟
downstream_bandwidth	入网带宽	该指标用于统计测试对象入云平台的网络速度（原指标为下行带宽）。	≥ 0	bit/s	1000(SI)	• bandwidth_id • publicip_id	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	维度	监控周期（原始指标）
upstream_bandwidth_usage	出网带宽使用率	该指标用于统计测量对象出云平台的带宽使用率。 出网带宽使用率=出网带宽指标/购买的带宽大小。	0-100	%	不涉及	• bandwidth_id • publicip_id	1分钟
downstream_bandwidth_usage	入网带宽使用率	该指标用于统计测量对象入云平台的带宽使用率。 入网带宽使用率=入网带宽指标/购买的带宽大小。 **说明** • 由于华为云在部分站点对10Mbps以下的配置带宽提供10Mbps的入网带宽上限，此时监控的入网带宽使用率会存在大于100%的情况。 • EIP使用时修改带宽大小，带宽使用率的指标同步生效会有5~10min的延时。	0-100	%	不涉及	• bandwidth_id • publicip_id	1分钟
up_stream	出网流量	该指标用于统计测试对象出云平台的网络流量（原指标为上行流量）。	≥ 0	Byte	1000(SI)	• bandwidth_id • publicip_id	1分钟

指标ID	指标名称	指标含义	取值范围	单位	进制	维度	监控周期（原始指标）
down_stream	入网流量	该指标用于统计测试对象入云平台的网络流量（原指标为下行流量）。	≥ 0	Byte	1000(SI)	• bandwidth_id • publicip_id	1分钟

维度

key	Value
publicip_id	弹性公网IP ID。
bandwidth_id	带宽ID。

4.4 支持的监控指标（终端入云 VPN）

功能说明

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

命名空间

SYS.VPN

监控指标

表 4-4 企业版 VPN 网关支持的监控指标

指标ID	指标名称	指标含义	取值范围	单位	进制	维度	监控周期（原始指标）
gateway_send_pkt_rate	出云包速率	该指标用于统计测量对象平均每秒出云的数据包数量。	≥ 0	pps	不涉及	p2c_vpn_gateway_id	1分钟
gateway_recv_pkt_rate	入云包速率	该指标用于统计测量对象平均每秒入云的数据包数量。	≥ 0	pps	不涉及	p2c_vpn_gateway_id	1分钟
gateway_send_rate	出云带宽	该指标用于统计测量对象平均每秒出云流量。	0-1	bps	1024(IEC)	p2c_vpn_gateway_id	1分钟
gateway_recv_rate	入云带宽	该指标用于统计测量对象平均每秒入云流量。	0-1	bps	1024(IEC)	p2c_vpn_gateway_id	1分钟
gateway_send_rate_usage	出云带宽使用率	该指标用于统计测量对象出云带宽使用率。	0-100	percentage(%)	不涉及	p2c_vpn_gateway_id	1分钟
gateway_recv_rate_usage	入云带宽使用率	该指标用于统计测量对象入云带宽使用率。	0-100	percentage(%)	不涉及	p2c_vpn_gateway_id	1分钟
gateway_connection_num	连接数	该指标用于统计测量对象关联VPN连接数。	≥ 0	count	不涉及	p2c_vpn_gateway_id	1分钟

维度

key	Value
p2c_vpn_gateway_id	企业版**终端入云VPN**网关。

4.5 支持的事件监控（站点入云 VPN 企业版）

功能说明

事件监控提供了事件类型数据上报、查询和告警的功能。用户可以通过云监控服务提供的管理控制台检索VPN服务产生的事件监控和告警信息。

命名空间

SYS.VPN

表 4-5 VPN 支持的事件监控

事件名称	事件ID	事件级别	事件说明	处理建议	事件影响
证书1天后过期	VPNCertificatePreExpire1Day	紧急	国密证书到期告警	请尽快更换证书	无
证书3天后过期	VPNCertificatePreExpire3Days	紧急	国密证书到期告警	请尽快更换证书	无
证书7天后过期	VPNCertificatePreExpire7Days	紧急	国密证书到期告警	请尽快更换证书	无
证书15天后过期	VPNCertificatePreExpire15Days	重要	国密证书到期告警	请尽快更换证书	无
证书30天后过期	VPNCertificatePreExpire30Days	重要	国密证书到期告警	请尽快更换证书	无
证书60天后过期	VPNCertificatePreExpire60Days	重要	国密证书到期告警	请尽快更换证书	无
证书已过期	VPNCertificateExpire	紧急	国密证书到期告警	请尽快更换证书	业务中断

4.6 查看监控指标

操作场景

查看VPN连接状态、带宽、弹性公网IP的使用情况。支持查看“近1小时”、“近3小时”、“近12小时”、“近24小时”、“近7天”或自定义时间段的数据。

背景信息

表 4-6 背景信息

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

查看 VPN 网关监控指标

- 通过虚拟专用网络入口
  a. 登录管理控制台。
  b. 在管理控制台左上角单击 图标，选择区域和项目。
  c. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
  d. 根据不同VPN类型查看监控指标。
     - 站点入云VPN企业版：选择“虚拟专用网络 > 企业版-VPN网关 > 站点入云VPN网关”，单击VPN网关对应“网关IP”列的 。支持对两个EIP分别进行监控指标查看。
       此处的监控指标为EIP监控指标，包括出网带宽、入网带宽、入网带宽使用率、出网带宽使用率、出网流量、入网流量。
     - 站点入云VPN经典版：选择“虚拟专用网络 > 经典版 > VPN网关”，单击VPN网关对应“操作”列的“查看监控”。系统会自动跳转到云监控服务页面。

此处的监控指标为EIP监控指标，包括出网带宽、入网带宽、入网带宽使用率、出网带宽使用率、出网流量、入网流量。

- 终端入云VPN：选择“虚拟专用网络 > 企业版-VPN网关 > 终端入云VPN网关”，单击VPN网关对应“网关IP”列的。
  此处的监控指标为EIP监控指标，包括出网带宽、入网带宽、入网带宽使用率、出网带宽使用率、出网流量、入网流量。

- 通过云监控服务入口
  a. 登录管理控制台。
  b. 在管理控制台左上角单击图标，选择区域和项目。
  c. 在页面左上角单击图标，选择“管理与监管> 云监控服务”。
  d. 选择“云服务监控 > 虚拟专用网络”。
  e. 根据不同VPN类型查看监控指标。
     - 站点入云VPN企业版：从下拉选项中选择“企业版站点入云VPN网关”。在“资源详情”页签，单击操作列的“查看监控指标”。
       此处的监控指标为VPN网关监控指标，包括出云包速率、入云带宽、出云带宽、入云带宽使用率、连接数、出云带宽使用率、入云包速率。
     - 终端入云VPN：从下拉选项中选择“企业版终端入云VPN网关”。在“资源详情”页签，单击操作列的“查看监控指标”。
       此处的监控指标为VPN网关监控指标，包括连接数、入云包速率、入云带宽、入云带宽使用率、出云带宽、出云包速率、出云带宽使用率。

查看 VPN 连接监控指标

- 通过虚拟专用网络入口
  a. 登录管理控制台。
  b. 在管理控制台左上角单击图标，选择区域和项目。
  c. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
  d. 根据不同VPN类型查看监控指标。
     - 站点入云VPN企业版：选择“虚拟专用网络 > 企业版-VPN连接”，单击VPN连接对应“监控”列的，查看监控。
       支持查看“近15分钟”、“近30分钟”、“近1小时”、“近2小时”、“近3小时”、“近12小时”、“近24小时”、“近7天”、“近30天”或自定义时间段的数据。
       监控指标包括：
       - 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
         以上指标需要开启健康检查项才会展现。单击VPN连接名称，在“基本信息”页签添加健康检查项。
       - 隧道往返平均时延、隧道往返最大时延、隧道丢包率
         以上指标仅VPN连接使用静态路由模式，且开启NQA检测机制场景时才会展现。

- 站点入云VPN经典版：选择“虚拟专用网络 > VPN连接”，单击VPN连接对应“操作”列的“更多 > 查看监控”。系统会自动跳转到云监控服务页面。

  监控指标包括VPN连接状态。

- 通过云监控服务入口

  a. 登录管理控制台。

  b. 在管理控制台左上角单击 图标，选择区域和项目。

  c. 在页面左上角单击图标，选择“管理与监管> 云监控服务”。

  d. 选择“云服务监控 > 虚拟专用网络”。

  e. 根据不同VPN类型查看监控指标。

  - 站点入云VPN企业版：

    1) 从下拉选项中选择“企业版站点入云VPN连接”。

    2) 在“资源详情”页签，单击操作列的“查看监控指标”，查看VPN连接监控指标。

    监控指标包括：

    - VPN连接状态、接收包速率、发送包速率、接收速率、发送速率

    - 链路往返平均时延、链路往返最大时延、链路丢包率

    以上指标需要开启健康检查项才会展现。单击VPN连接名称，在“基本信息”页签添加健康检查项。

    - 隧道往返平均时延、隧道往返最大时延、隧道丢包率

    以上指标仅VPN连接使用静态路由模式，且开启NQA检测机制场景时才会展现。

  - 站点入云VPN经典版：从下拉选项中选择“VPN连接”。在“资源详情”页签，单击操作列的“查看监控指标”。

    监控指标包括VPN连接状态。

4.7 创建监控告警规则

操作场景

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

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“管理与监管> 云监控服务”。
4. 选择“云服务监控 > 虚拟专用网络 VPN”，根据不同告警类型在不同页签下配置告警规则。

- 站点入云VPN企业版对应的VPN网关告警，请从下拉选项中选择“企业版站点入云VPN网关”。在“资源详情”页签，选择操作列的“更多 > 创建告警规则”进行配置。
- 站点入云VPN企业版对应的VPN连接告警，请从下拉选项中选择“企业版站点入云VPN连接”。在“资源详情”页签，选择操作列的“更多 > 创建告警规则”进行配置。
- 终端入云VPN对应的VPN网关告警，请从下拉选项中选择“企业版终端入云VPN网关”。在“资源详情”页签，选择操作列的“更多 > 创建告警规则”进行配置。
- 站点入云VPN经典版对应的VPN连接的告警，请从下拉选项中选择“VPN连接”。在“资源详情”页签，选择操作列的“更多 > 创建告警规则”进行配置。

5. 配置告警规则。
   - 关联模板：系统默认提供告警模板“虚拟专用网络默认告警模板（VPN连接）”，可以直接关联使用。
   - 自定义创建：如果需要对告警策略进行定制，请单击“自定义创建”进行创建。创建完成后，该策略可以在关联模板中使用。
6. 规则参数设置完成后，单击“立即创建”。

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

   说明

   更多关于虚拟专用网络监控规则的信息，请参见**《云监控用户指南》**。

4.8 创建事件告警规则

操作场景

通过设置事件告警规则，用户可自定义事件监控范围与通知策略，及时了解虚拟专用网络的状况，从而起到预警作用。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在管理控制台左上角单击，选择“管理与监管 > 云监控服务”。
4. 单击“事件监控”，进入“事件监控”页面。
5. 在页面右上方，单击“创建告警规则”，进入“创建告警规则”页面。
6. 配置事件告警规则。请参考**表 告警参数**。

表 4-7 告警参数

参数	说明
名称	系统会自动生成一个名称，也可以自定义修改。
告警类型	选择“事件”。

参数	说明
事件类型	选择“系统事件”。
事件来源	选择“虚拟专用网络”。
监控范围	全部资源。
触发规则	根据实际需要选择。
告警策略	推荐选择“证书1天后过期”、“证书3天后过期”、“证书7天后过期”。当证书即将到期时，系统会在到期前7天、到期前3天、到期前1天各发送一次告警通知。
通知方式	根据实际选择进行配置。 **说明** 告警消息由消息通知服务SMN发送，可能产生少量费用。

7. 规则参数设置完成后，单击“立即创建”。

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

5 审计

5.1 支持审计的关键操作列表

说明

站点入云VPN经典版墨西哥城一/圣保罗一Region不支持云审计服务。

表 5-1 站点入云 VPN 企业版操作列表

操作名称	资源类型	事件名称
创建用户对端网关	customer-gateway	createCgw
更新用户对端网关	customer-gateway	updateCgw
删除用户对端网关	customer-gateway	deleteCgw
创建虚拟专用网络网关	vpn-gateway	createVgw
更新虚拟专用网络网关	vpn-gateway	updateVgw
删除虚拟专用网络网关	vpn-gateway	deleteVgw
包年/包月创建VPN网关	vpn-gateway	createPrePaidVgw
更新VPN网关状态	vpn-gateway	updateResourceState
更新包周期VPN网关规格	vpn-gateway	updateVgwSpecification
更新按需VPN网关规格	vpn-gateway	updatePostpaidVgwSpecification

操作名称	资源类型	事件名称
创建虚拟专用网络连接	vpn-connection	createVpnConnection
更新虚拟专用网络连接	vpn-connection	updateVpnConnection
删除虚拟专用网络连接	vpn-connection	deleteVpnConnection
上传网关证书	vgw-certificate	createVgwCertificate
更换网关证书	vgw-certificate	updateVgwCertificate
创建资源标签	instance	batchCreateResourceTags
删除资源标签	instance	batchDeleteResourceTags
查询用户对端网关列表	customer-gateway	listCgws
查询用户对端网关	customer-gateway	showCgw
查询资源标签	instance	showResourceTags
查询项目标签	instance	listProjectTags
按标签查询资源实例列表	instance	listResourcesByTags
按标签查询资源实例数量	instance	countResourcesByTags
查询VPN网关证书	vpn-gateway	showVpnGatewayCertificate
查询VPN网关	vpn-gateway	showVgw
查询VPN网关可用区	availability_zone	listAvailabilityZones
查询VPN网关可用区	availability_zone	listExtendedAvailabilityZones
查询指定VPN网关下的路由表	vpn-gateway	showVpnGatewayRoutingTable
查询VPN连接列表	vpn-connection	listVpnConnections
查询VPN连接	vpn-connection	showVpnConnection
查询VPN网关列表	vpn-gateway	listVgws
查询VPN连接监控	connection-monitor	showConnectionMonitor
查询VPN连接监控列表	connection-monitor	listConnectionMonitors

操作名称	资源类型	事件名称
查询指定租户配额	quota	showQuotasInfo
查询VPN连接日志	vpn-connection	showVpnConnectionLog
批量创建VPN连接	vpn-connection	batchCreateVpnConnection
重置VPN连接	vpn-connection	resetVpnConnection
升级站点入云VPN网关	vpn-gateway	upgradeVpnGateway
查询站点入云VPN网关任务列表	vpn-gateway	listVpnGatewayJobs
删除站点入云VPN网关任务	vpn-gateway	deleteVpnGatewayJob
创建VPN连接监控	connection-monitor	createConnectionMonitor
删除VPN连接监控	connection-monitor	deleteConnectionMonitor

表 5-2 站点入云 VPN 经典版操作列表

操作名称	资源类型	事件名称
创建vpn连接	VpnConnection	createVpnConnection
更新vpn连接	VpnConnection	updateVpnConnection
删除vpn连接	VpnConnection	deleteVpnConnection
创建vpn网关	VpnGw	createVpnGw
更新vpn网关	VpnGw	updateVpnGw
删除vpn网关	VpnGw	deleteVpnGw
查询VPN连接	VpnConnection	showVpnConnection
查询VPN连接列表	VpnConnection	listVpnConnection
查询IPSEC策略		
查询IKE策略		
查询VPN网关	VpnGw	showVpnGw
查询VPN网关列表	VpnGw	listVpnGw
查询配额	quota	showQuota
查询国密算法列表	VpnConnection	listSupportedAlgorithm

表 5-3 终端入云 VPN 操作列表

操作名称	资源类型	事件名称
订购资源	p2c-vpn-gateway	subscribeP2cVgw
更新包周期VPN网关规格	p2c-vpn-gateway	updateP2cVgwSpecification
资源状态变更（冻结解冻）	p2c-vpn-gateway	updateP2cVgwStatus
退订资源	p2c-vpn-gateway	unsubscribeP2cVgw
创建终端入云VPN网关	p2c-vpn-gateway	createP2cVgw
更新终端入云VPN网关	p2c-vpn-gateway	updateP2cVgw
删除终端入云VPN网关	p2c-vpn-gateway	deleteP2cVgw
创建SSL服务端	vpn-server	createVpnServer
修改SSL服务端	vpn-server	updateVpnServer
创建VPN用户	vpn-user	createVpnUser
修改VPN用户	vpn-user	updateVpnUser
修改VPN用户密码	vpn-user	updateVpnUserPassword
重置VPN用户密码	vpn-user	resetVpnUserPassword
删除VPN用户	vpn-user	deleteVpnUser
创建VPN用户组	vpn-user-group	createVpnUserGroup
修改VPN用户组	vpn-user-group	updateVpnUserGroup
添加VPN用户组用户	vpn-user-group	addVpnUsersToGroup
移除VPN用户组用户	vpn-user-group	removeVpnUsersToGroup
创建VPN访问策略	vpn-access-policy	createVpnAccessPolicy
修改VPN访问策略	vpn-access-policy	updateVpnAccessPolicy
删除VPN访问策略	vpn-access-policy	deleteVpnAccessPolicy
下载客户端配置	vpn-server	exportClientConfig

操作名称	资源类型	事件名称
导入客户端CA证书	client-ca-certificate	importClientCa
修改客户端CA证书	client-ca-certificate	updateClientCa
删除客户端CA证书	client-ca-certificate	deleteClientCa
批量创建资源标签	p2c-vpn-gateway	batchCreateResourceTags
批量删除资源标签	p2c-vpn-gateway	batchDeleteResourceTags
查询终端入云VPN网关列表	p2c-vpn-gateway	listP2cVgws
根据终端入云VPN网关ID，查询指定的VPN网关	p2c-vpn-gateway	showP2cVgw
查询终端入云VPN网关可用区	p2c-vpn-gateway	listP2cVgwAvailabilityZones
查询终端入云VPN网关连接信息列表	p2c-vpn-gateway	listP2cVgwConnections
查询指定实例的标签信息	p2c-vpn-gateway	listTagsForResource
查询租户在指定Project中实例类型的所有资源标签集合	p2c-vpn-gateway	listTags
查询VPN访问策略列表	vpn-access-policy	listVpnAccessPolicies
查询VPN访问策略	vpn-access-policy	showVpnAccessPolicy
查询一个网关下的服务端信息	vpn-server	listVpnServersByVgw
查询客户端CA证书	client-ca-certificate	showClientCa
查询租户下的所有服务端信息	vpn-server	listVpnServersByProject
查询VPN用户列表	vpn-user	listVpnUsers
查询VPN用户	vpn-user	showVpnUser

操作名称	资源类型	事件名称
查询VPN用户组列表	vpn-user	listVpnUserGroups
查询VPN用户组	vpn-user	showVpnUserGroup
查询组内VPN用户	vpn-user	listVpnUsersInGroup
批量创建VPN用户	vpn-user	batchCreateVpnUsers
批量删除VPN用户	vpn-user	batchDeleteVpnUsers
创建/更新连接日志配置	p2c-vpn-gateway	updateVpnConnectionsLogConfig
删除连接日志配置	p2c-vpn-gateway	deleteVpnConnectionsLogConfig
查询连接日志配置	p2c-vpn-gateway	showVpnConnectionsLogConfig
断开终端入云VPN网关连接	p2c-vpn-gateway	disconnectP2cVgwConnection
升级终端入云VPN网关	p2c-vpn-gateway	upgradeP2cVpnGateway
查询终端入云VPN网关任务列表	p2c-vpn-gateway	listP2cVpnGatewayJobs
删除终端入云VPN网关任务	p2c-vpn-gateway	deleteP2cVpnGatewayJob
单点登录终端入云VPN	p2c-vpn-gateway	loginP2cVpnBySSO

5.2 查看云审计日志

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

相关链接：

如何查看审计日志，请参见**查看审计日志**。

6 权限管理

6.1 创建用户并授权使用 VPN

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

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

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

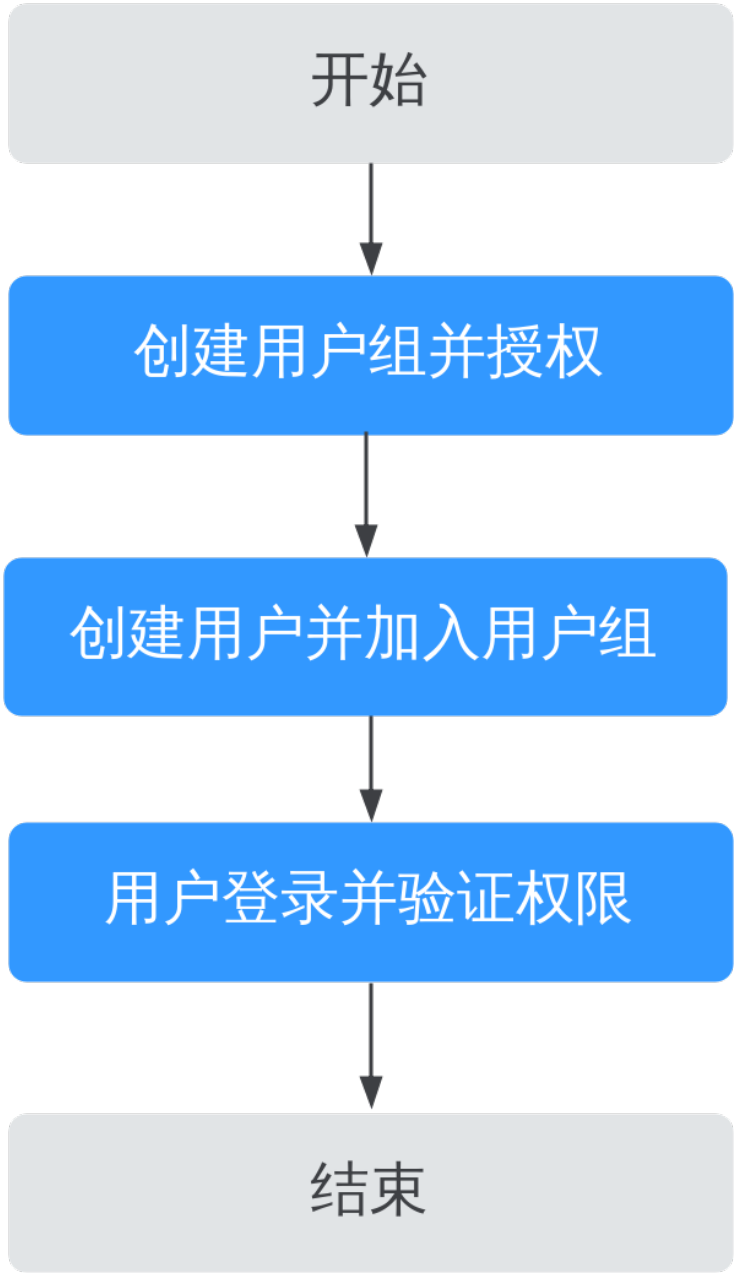
本章节为您介绍对用户授权的方法，操作流程如**图6-1**所示。

前提条件

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

示例流程

图 6-1 给用户授予 VPN 权限流程



1. **创建用户组并授权**
   在IAM控制台创建用户组，并授予虚拟专用网络服务权限“VPN FullAccess”。
2. **创建用户并加入用户组**
   在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限。
   新创建的用户登录管理控制台，切换至授权区域，验证权限：
   - 在页面左上角单击图标，选择“网络 > 虚拟专用网络 > ”，进入“虚拟专用网络 > 企业版-VPN网关”页面，在“站点入云VPN网关”页签，单击

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

- 在页面左上角单击  图标，选择“网络 > 虚拟专用网络”，进入“虚拟专用网络 > 经典版”页面，单击“创建VPN网关”，尝试创建VPN网关，如果创建成功，表示“VPN FullAccess”已生效。
- 在页面左上角单击  图标，选择“网络 > 虚拟专用网络”，进入“虚拟专用网络 > 企业版-VPN网关”页面，单击“终端入云VPN网关”，进入“终端入云VPN网关”页签，单击右上角“创建终端入云VPN网关”，尝试创建VPN网关，如果创建成功，表示“VPN FullAccess”已生效。
- 在页面左上角单击  图标，选择除VPN服务外（假设当前权限仅包含VPN FullAccess）的任一服务，若提示权限不足，表示“VPN FullAccess”已生效。

6.2 VPN 自定义策略

如果系统预置的VPN权限，不满足您的授权要求，可以创建自定义策略。

目前华为云支持以下两种方式创建自定义策略：

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

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的VPN自定义策略样例。

VPN 自定义策略样例

- 示例1：授权用户删除VPN网关

  需要添加如下依赖的授权项，如果不添加依赖的授权项，可能会出现异常。

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

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "er:instances:get",
                "er:instances:list"
            ]
        }
    ]
}
```

- 示例2：拒绝用户删除VPN连接

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

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

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

- 示例3：多个授权项策略

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

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

7 标签管理

7.1 应用场景

VPN标签是VPN资源的标识。为VPN资源添加标签，可以方便用户识别和管理拥有的VPN。您可以在创建VPN资源的时候增加标签，或者在已经创建的VPN资源详情页添加标签，每个VPN资源最多可以添加20个标签。

说明

VPN标签管理仅支持站点入云VPN企业版和终端入云VPN。

标签共由两部分组成：“键”和“值”，其中，“键”和“值”的命名规则如**表 VPN标签命名规则**所示。

表 7-1 VPN 标签命名规则

参数	规则	样例
键	• 不能为空。 • 对于同一虚拟专用网络键值唯一。 • 长度不超过128个字符。 • 只能包含以下几种字符： – 数字 – 空格 – 任意语种字母 – 特殊字符，包括“_”、“.”、“:”、“=”、“+”、“-”和“@” • 首尾不能含有空格，不能以_sys_开头。	vpn_key1

参数	规则	样例
值	• 长度不超过255个字符。 • 只能包含以下几种字符： – 数字 – 空格 – 任意语种字母 – 特殊字符，包括“_”、"."、“:”、“/”、“=”、“+”、“-”、“@”	vpn-01

7.2 站点入云 VPN 企业版

7.2.1 标签搜索

背景信息

对已增加的标签键和标签值进行搜索，包括VPN网关、对端网关和VPN连接。

操作步骤

站点入云VPN企业版VPN网关搜索标签。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 单击“站点入云VPN网关”进入“站点入云VPN网关”页面。
6. 在“站点入云VPN网关”页面，单击搜索框“选择属性筛选，或输入关键字搜索”，选择“资源标签 ”，添加筛选条件标签键值。

   系统根据标签键和标签值来搜索目标VPN网关。

   – 此查询功能仅支持选择下拉列表中已存在的键和值。
   – 支持多个不同标签组合搜索。如果输入多个标签，则不同标签之间为“与”的关系。
   – 支持标签和其他条件进行组合搜索。标签和其他搜索条件组合的搜索也是“与”的关系。

站点入云VPN企业版对端网关搜索标签。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。

4. 在左侧导航栏，单击虚拟专用网络企业版-对端网关”。
5. 单击搜索框“选择属性筛选，或输入关键字搜索”，选择“资源标签 ”，添加筛选条件标签键值。

   系统根据标签键和标签值来搜索目标对端网关。

   - 此查询功能仅支持选择下拉列表中已存在的键和值。
   - 支持多个不同标签组合搜索。如果输入多个标签，则不同标签之间为“与”的关系。
   - 支持标签和其他条件进行组合搜索。标签和其他搜索条件组合的搜索也是“与”的关系。

站点入云VPN企业版VPN连接搜索标签。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，单击虚拟专用网络企业版-VPN连接”。
5. 单击搜索框“选择属性筛选，或输入关键字搜索”，选择“资源标签 ”，添加筛选条件标签键值。

   系统根据标签键和标签值来搜索VPN连接。

   - 此查询功能仅支持选择下拉列表中已存在的键和值。
   - 支持多个不同标签组合搜索。如果输入多个标签，则不同标签之间为“与”的关系。
   - 支持标签和其他条件进行组合搜索。标签和其他搜索条件组合的搜索也是“与”的关系。

经典版VPN网关搜索标签。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，单击“虚拟专用网络 > 经典版”。
5. 在“经典版”界面，单击右上角“标签搜索”，选择对应标签键值，然后单击“搜索”。
   - 此查询功能仅支持选择标签列表中已存在的键和值。
   - 支持最多20个不同标签的组合搜索。

7.2.2 标签管理

背景信息

对目标VPN资源进行标签管理，包括增、删、改、查的操作。

操作步骤

站点入云VPN企业版VPN网关标签管理操作。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 单击“站点入云VPN网关”进入“站点入云VPN网关”页面。
6. 选择目标VPN网关，单击VPN网关的名称，进入VPN网关详情页。
7. 选择“标签”页签，可以对VPN网关的标签进行增、删、改、查。
   - 添加

     单击“添加”，在弹出的“添加标签”窗口，输入新添加标签的键和值，并单击“确定”。
   - 修改

     单击标签所在行“操作”列下的“编辑”，在弹出的“编辑标签”窗口，输入修改后标签的值，并单击“确定”。
   - 删除

     单击标签所在行“操作”列下的“删除”，在弹出的“删除标签”窗口，单击“确定”。
   - 查看。

     在“标签”页签，可以查看“标签”详情，包括剩余可创建的标签个数，以及每个标签的键和值。

站点入云VPN企业版对端网关标签管理操作。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-对端网关”。
5. 选择目标对端网关，单击对端网关的名称，进入对端网关详情页。
6. 选择“标签”，可以对对端网关的标签进行增、删、改、查。
   - 添加

     单击“添加”，在弹出的“添加标签”窗口，输入新添加标签的键和值，并单击“确定”。
   - 修改

     单击标签所在行“操作”列下的“编辑”，在弹出的“编辑标签”窗口，输入修改后标签的值，并单击“确定”。
   - 删除

     单击标签所在行“操作”列下的“删除”，在弹出的“删除标签”窗口，单击“确定”。
   - 查看。

     在对端网关详情页的“标签”，可以查看“标签”详情，包括剩余可创建的标签个数，以及每个标签的键和值。

站点入云VPN企业版VPN连接标签管理操作。

1. 登录管理控制台。

2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN连接”。
5. 选择目标VPN连接，单击VPN连接的名称，进入VPN连接详情页。
6. 选择“标签”页签，可以对VPN连接的标签进行增、删、改、查。
   - 添加

     单击“添加”，在弹出的“添加标签”窗口，输入新添加标签的键和值，并单击“确定”。
   - 修改

     单击标签所在行“操作”列下的“编辑”，在弹出的“编辑标签”窗口，输入修改后标签的值，并单击“确定”。
   - 删除

     单击标签所在行“操作”列下的“删除”，在弹出的“删除标签”窗口，单击“确定”。
   - 查看。

     在“标签”页签，可以查看“标签”详情，包括剩余可创建的标签个数，以及每个标签的键和值。

经典版VPN网关标签管理操作。

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，单击“虚拟专用网络 > 经典版”。
5. 在“经典版”界面，选择目标VPN网关，单击VPN网关的名称，进入VPN网关详情页。
6. 选择“标签”页签，可以对VPN网关的标签进行增、删、改、查。
   - 添加

     单击左上角的“添加”，在弹出的“添加标签”窗口，输入新添加标签的键和值，并单击“确定”。
   - 修改

     单击标签所在行“操作”列下的“编辑”，在弹出的“编辑标签”窗口，输入修改后标签的值，并单击“确定”。
   - 删除

     单击标签所在行“操作”列下的“删除”，在弹出的“确定要对以下标签进行删除操作吗”窗口，单击“确定”。
   - 查看。

     在“标签”页签，可以查看当前虚拟专用网络的标签详情，包括剩余可创建的标签个数，以及每个标签的键和值。

7.3 终端入云 VPN

7.3.1 标签搜索

背景信息

对VPN网关已增加的标签键和标签值进行搜索。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 单击“终端入云VPN网关”进入“终端入云VPN网关”页面。
6. 在“终端入云VPN网关”页面，单击“选择属性筛选，或输入关键字搜索”，选择“资源标签”，添加筛选条件标签键值，搜索目标VPN网关。
   - 此查询功能仅支持选择标签列表中已存在的键和值。
   - 支持多个不同标签组合搜索。如果输入多个标签，则不同标签之间为“或”的关系。
   - 支持标签和其他条件进行组合搜索。标签和其他搜索条件组合的搜索也是“或”的关系。

7.3.2 标签管理

背景信息

对目标VPN资源进行标签管理，包括增、删、改、查的操作。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在页面左上角单击图标，选择“网络 > 虚拟专用网络 VPN”。
4. 在左侧导航栏，选择“虚拟专用网络 > 企业版-VPN网关”。
5. 单击“终端入云VPN网关”进入“终端入云VPN网关”页面。
6. 选择目标VPN网关，单击VPN网关的名称，进入VPN网关详情页。
7. 选择“标签”页签，可以对VPN网关的标签进行增、删、改、查。
   - 添加

     单击“添加”，在弹出的“添加标签”窗口，输入新添加标签的键和值，并单击“确定”。
   - 修改

     单击标签所在行“操作”列下的“编辑”，在弹出的“编辑标签”窗口，输入修改后标签的值，并单击“确定”。
   - 删除

     单击标签所在行“操作”列下的“删除”，在弹出的“确定要对以下标签进行删除操作吗”窗口，单击“确定”。

- 查看。

  在“标签”页签，可以查看“标签”详情，包括剩余可创建的标签个数，以及每个标签的键和值。

8 关于配额

什么是配额?

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

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

资源类型

- 站点入云VPN经典版的资源类型包括经典版VPN网关和经典版VPN连接。
- 站点入云VPN企业版的资源类型包括VPN网关、VPN连接组和对端网关。
- 终端入云VPN的资源类型仅支持VPN网关。

资源类型的总配额根据部署Region存在差异，请以实际部署环境为准。

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”。
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”。
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”。

