VPN连接（VPN）

产品文档

目录

产品简介
产品概述

VPN 连接是通过公网加密通道实现远程访问的一种方式。VPN网关是VPN连接的重要组成部分，目前有两种VPN网关类型：

- IPsec VPN网关：主要实现site to site的互联互通。例如，IDC与私有网络（Virtual Private Cloud，VPC）连接，在建立 VPN 连接后，您只需要在路由表中配置相关路由策略，即可实现通信。如下图所示， IPsec VPN 连接分为如下组成部分：
- VPN 网关：在VPC内创建的 IPsec VPN 网关。
- 对端网关：记录IDC端IPsec VPN网关公网IP地址的逻辑对象（IDC端必须有固定公网 IP）。
- VPN 通道：一条连接VPN网关和对端网关的加密的IPsec VPN通道， 每个VPN网关可以建立多个VPN通道，每个VPN通道可以打通一个本地IDC。

- SSL VPN网关：主要实现点到点的互联互通。例如，您可以通过任何内嵌SSL的浏览器，访问VPN服务器，从而实现对VPC的访问。如下图所示，SSL VPN连接分为如下组成部分。
- VPN网关：在VPC内创建的SSL VPN网关。
- SSL服务端：VPN网关中用于提供SSL服务的服务模块，主要实现数据包的封装与解封装。
- SSL客户端：可以通过任何内嵌SSL的浏览器作为SSL客户端进行访问。

产品组成
IPsec VPN

VPN连接支持IPsec VPN和SSL VPN连接，本章节介绍两种连接方式的组成。

IPsec VPN

IPsec VPN 连接有三个组成部分：VPN 网关、对端网关、VPN 通道。

VPN网关

VPN 网关是 VPC 建立 VPN 连接的出口网关，与对端网关（IDC 侧的 IPsec VPN 服务网关）配合使用，主要用于云平台 VPC 和外部 IDC 之间建立安全可靠的加密网络通信。 VPN 网关通过软件虚拟化处理，采用双机热备策略，单台故障时自动切换，不影响业务正常运行。

VPN 网关带宽上限分为8种：5M、10M、20M、50M、100M，单位为bps。

对端网关

对端网关是用来记录 IDC 端的 IPsec VPN 网关公网 IP 地址的逻辑对象（IDC 端必须有固定公网 IP），需与 VPN 网关配合使用，一个 VPN 网关可与多个对端网关建立加密的 VPN 网络通道。

VPN 通道

VPN 网关和对端网关建立后，即可建立用于 VPC 与外部 IDC 之间加密通信的 VPN 通道。该VPN通道支持 IPsec 加密协议，可满足绝大多数 VPN 连接的需求。
VPN 通道在运营商公网中运行，公网的网络阻塞、抖动会影响 VPN 网络质量。若业务对延时、抖动敏感，建议您通过专线接入 VPC，更多详情，请参见专线接入服务。

建立 VPN 通道

云平台中的 VPN 通道在实现 IPsec 时，使用 IKE（Internet Key Exchange，因特网密钥交换）协议来建立会话。
IKE 具有一套自我保护机制，可以在不安全的网络上安全地认证身份、分发密钥、建立 IPSec 会话。
VPN 通道的建立包括以下配置信息：

- 基本配置
- SPD（Security Policy Database）策略
- IKE 配置（选填）
- IPsec 配置（选填）

下面将详细介绍基本信息、SPD 策略、IKE 配置（选填）和 IPsec 配置（选填）。

基本配置

基本配置中主要包括VPN通道名称、所属地域、私有网络及VPN网关、对端网关等基本信息。

SPD 策略

SPD（Security Policy Database）策略由一系列 SPD 规则组成，用于指定 VPC 内哪些网段可以和 IDC 内哪些网段通信。每条 SPD 规则包括一个本端网段 CIDR，和至少一个对端网段 CIDR。一个本端网段CIDR和一个对端网段CIDR构成一组匹配关系。一个SPD规则下可以有多组匹配关系。

> 说明：
>
> 同一 VPN 网关下所有通道内的规则，匹配关系不能重叠，即一组的匹配关系中，本端网段和对端网段不能同时重叠。

示例：
如下图所示，某 VPN 网关下已经存在以下 SPD 规则：

- SPD 规则1本端网段 10.0.0.0/24，对端网段为 192.168.0.0/24、192.168.1.0/24，有两组匹配关系。
- SPD 规则2本端网段 10.0.1.0/24，对端网段为 192.168.2.0/24，有一组匹配关系。
- SPD 规则3本端网段 10.0.2.0/24，对端网段为 192.168.2.0/24，有一组匹配关系。

他们的匹配关系分别是：

- 10.0.0.0/24-----192.168.0.0/24
- 10.0.0.0/24-----192.168.1.0/24
- 10.0.1.0/24-----192.168.2.0/24
- 10.0.2.0/24-----192.168.2.0/24

这四组匹配关系相互不能重叠，即他们的本端网段和对端网段不能同时重叠。

- 如果新增一个10.0.0.0/24-----192.168.1.0/24匹配关系，则会因为和已有匹配关系重叠，而无法添加 SPD 规则。
- 如果新增一个10.0.1.0/24-----192.168.1.0/24匹配关系，和已有的3个匹配关系均不重叠，则可以加入 SPD 规则。

IKE 配置

配置项	说明
版本	IKE V1
身份认证方法	默认预共享密钥
认证算法	身份认证算法，支持 MD5 和 SHA1
协商模式	支持 main（主模式）和 aggressive（野蛮模式） 二者的不同之处在于，aggressive 模式可以用更少的包发送更多信息，可以快速建立连接，但是

配置项	说明
	是以清晰的方式发送安全网关的身份。使用 aggressive 模式时，配置参数如 Diffie-Hellman 和 PFS 不能进行协商，要求两端拥有兼容的配置
本端标识	支持 IP address 和 FQDN（全称域名）
对端标识	支持 IP address 和 FQDN
DH group	指定 IKE 交换密钥时使用的 DH 组，密钥交换的安全性随着 DH 组的扩大而增加，但交换的时间也增加了 • Group1：采用 768-bit 模指数（Modular Exponential，MODP ）算法的 DH 组 • Group2：采用 1024-bit MODP 算法的 DH 组 • Group5：采用 1536-bit MODP 算法的 DH 组 • Group14：采用 2048-bit MODP 算法，不支持动态 VPN 实现此选项 • Group24：带 256 位的素数阶子群的 2048-bit MODP算法 DH 组，不支持组 VPN 实现此选项
IKE SA Lifetime	单位：秒 设置 IKE 安全提议的 SA 生存周期，在设定的生存周期超时前，会提前协商另一个 SA 来替换旧的 SA。在新的 SA 还没有协商完之前，依然使用旧的 SA；在新的 SA 建立后，将立即使用新的 SA，而旧的 SA 在生存周期超时后，被自动清除

IPsec 配置

配置项	说明
加密算法	支持 3DES、AES-128、AES-192、AES-256、DES
认证算法	支持 MD5 和 SHA1
报文封装模式	Tunnel
安全协议	ESP
PFS	支持 disable、dh-group2、dh-group5和dh-group14
IPsec SA lifetime(s)	单位：秒
IPsec SA lifetime(KB)	单位：KB

SSL VPN

SSL VPN

SSL VPN连接有三个部分组成：VPN网关、SSL服务端、SSL客户端。
实现原理：在VPC中创建SSL VPN网关实例，然后对VPN网关进行SSL服务端配置，再创建SSL服务端对应的SSL客户端，从而实现SSL客户端与VPC的通信。

VPN网关

VPN网关是VPC建立VPN连接的出口网关，客户端通过SSL VPN实现与VPC的通信。

SSL服务端

SSL服务端是VPN网关中用于提供SSL服务的服务模块，主要实现数据包的封装与解封装，因此需要在VPN网关中进行SSL 服务端的相关配置，如配置本端网段、客户端网段、以及通信协议、端口及算法等。

SSL客户端

SSL客户端采用OpenVPN对接，创建SSL客户端，并提供对应的客户端配置文件和证书的下载功能，客户端和服务器端需要进行双向认证，只有通过认证的客户端才可与服务端建立通信连接。
您可以通过任何内嵌SSL的浏览器作为SSL客户端进行访问。客户端操作系统支持Windows，MAC, Linux (主流版本）。

产品功能

远程通信

通过VPN连接可建立到VPC的远程通信，如通过IPsec VPN可打通IDC到VPC的site to site模式的互通；通过SSL VPN可建立客户端到VPC点到点的互通。具体实现方式可参见【快速入门】。

流量告警

您可以为 VPN 连接设置自定义流量告警，当指标超过一定阈值时自动告警，告警消息会通过电子邮件和短信发出，帮助您提前预警风险。监控和告警服务无需额外收费，同时当故障发生时，能帮助您快速定位问题。设置告警策略，详情请参见 设置告警。

指标监控

VPN网关支持数据监控功能，监控项主要包含外网出带宽、外网入带宽、出包量、入包量。
通过对各项指标的实时监控，您可以及时了解产品运行状态，保障产品稳定运行。

使用限制

IPsec VPN使用限制

使用 IPsec VPN 连接时，您需要注意如下几点：

- VPN 参数配置完成后，您需要在子网关联路由表中添加指向 VPN 网关的路由策略，子网内云服务器访问对端网段的网络请求才会通过 VPN 通道传递至对端网关。
- 在配置完路由表之后，您需要在 VPC 内云服务器 ping 对端网段中的 IP 以激活此 VPN 通道。
- VPN 连接稳定性依赖运营商公网质量。
- 资源限制如下：

资源	限制（个）	可申请高配额
每个 VPC 内 VPN 网关个数	10	否
同一地域内对端网关个数	20	否
同一个对端网关支持的 VPN 通道数	10	否
同一 VPN 网关可创建的 VPN 通道数	20	否
每个 VPN 通道的 SPD 个数	10	否
每个 SPD 支持的对端网段数	50	否

> 说明：
>
> - 同一个对端网关支持的 VPN 通道数为账户级配额。
> - 同一个对端网关与一个 VPC 内的同一个 VPN 网关仅可建立一个 VPN 通道。

对端网关不支持如下 IP 地址：

- 全0，全255，224开头的组播地址。
- 回环地址： 127.x.x.x/8 。
- IP 地址中主机位为全0或者全1的地址，例如：

- 以 A 类中1 - 126开头举例， 1 - 126.0.0.0 以及 1 - 126.255.255.255 。
- 以 B 类中128 - 191开头举例， 128 - 191.x.0.0 以及 128 - 191.x.255.255 。
- 以 C 类中192 - 223开头举例， 192 - 223.x.x.0 以及 192 - 223.x.x.255 。

- 内部服务地址： 169.254.x.x/16 。

SSL VPN 使用限制

SSL客户端约束：

- SSL VPN客户端使用开源OpenVPN做对接，OpenVPN需要用户自行下载。
- SSL VPN客户端必须要支持Windows，Mac， Linux（主流版本）系统。
- 客户端和服务端必须进行双向证书认证，客户端的证书和密钥都由云上申请和下载，提供配置文件的下载。
- 客户端证书SNI即是SSL VPN实例ID（SSL VPN客户端实例ID）。

SSL服务端约束：

- 服务端必须进行双向证书认证，根证书和服务端证书有效期为10年，客户端证书有效期为3年。
- 只能配置1个客户端IP地址池。
- 可访问1个VPC侧CIDR。
- 最大连接数，支持5、10、20、50、20、100。

SSL VPN网关约束：

- 客户端通过SSL VPN网关与VPC内VM通信，SSL VPN目前只对接OpenVPN客户端。
- EIP对外开放UDP 1194端口对外提供SSL VPN服务。
- 不同用户使用同一个证书和密钥与SSL VPN网关通信时，同一证书在同一时间只能有一个用户与SSL VPN网关建立SSL VPN连接，如果两个用户不停建连的情况下，会导致两个用户都不能建连。

相关产品

VPN 连接相关产品信息，请参见下表：

产品名称	与 VPN 连接的关系
私有网络	VPN 连接是一种通过公网加密通道连接您对端 IDC 和私有网络的方式。
专线接入	若业务对延时、抖动敏感，建议通过专线接入私有网络。
路由表	需要在子网所关联的路由表中，添加指向 IPsec VPN 网关的路由策略，网络请求才会通过 VPN 通道传递至对端网关。

购买指南
计费概述

IPsec VPN 连接由三部分组成：VPN 通道、对端网关和 VPN 网关，本文为您介绍各组成部分的计费详情。

VPN 通道

VPN 通道供用户免费使用。

对端网关

对端网关供用户免费使用。

VPN 网关

VPN 网关支持按流量计费，按流量计费为后付费模式，包含两部分费用：访问公网产生的流量费用和网关费用（按小时计算）。

网关询价

您可以在VPN网关购买页面，选择不同的带宽规格，了解相应的网关费用。

购买方式

下面将为您介绍购买 VPN 连接的具体操作。

1. 登录云平台，选择【云产品】>【云计算与网络】>【私有网络(VPC)】进入私有网络控制台。
2. 在左侧目录中单击【VPN连接】>【VPN网关】，进入【VPN网关】管理界面。
3. 选择地域，如示例中的广州，单击【新建】。
4. 在弹出的对话框中配置如下参数，单击【创建】即可。

- 网关名称：填写 VPN 网关名称，不超过60个字符。
- 所属网络：按需选择 VPN 网关的所属VPC网络。
- 带宽上限：按需选择 VPN 网关的带宽上限。

快速入门
创建IPsec VPN连接
入门概述

您需要完成几个步骤使 IPsec VPN 连接生效，之后可以在控制台实现IPsec VPN 全自助配置，下文将为您举例说明。

示例

通过 IPsec VPN 连接，打通您在广州的私有网络 TomVPC 中的子网 A（ 192.168.1.0/24 ）与您 IDC 中的子网（ 10.0.1.0/24 ）的通信，假设您 IDC 中 VPN 网关的公网 IP 为 202.108.22.5 。

步骤说明

VPN 连接激活流程图如下所示。

具体操作请参见：

- 步骤1：创建 VPN 网关
- 步骤2：创建对端网关
- 步骤3：创建 VPN 通道
- 步骤4：本地网关配置
- 步骤5：配置路由表
- 步骤6：激活 VPN 隧道

步骤1：创建 VPN 网关

1. 登录云平台，选择【云产品】>【云计算与网络】>【私有网络(VPC)】进入私有网络控制台。

2. 在左侧目录中单击【VPN连接】>【VPN网关】，进入【VPN网关】管理界面。

3. 选择地域，如示例中的广州，单击【新建】。

   > 说明： 若【新建】显示灰色，且鼠标移至上方时显示“无可用私有网络”，请 创建私有网络 后再进行新建 VPN 网关。

4. 在弹出的【新建VPN网关】对话框中，填写 VPN 网关名称（如 TomVPNGw），选择所属网络、带宽上限，VPN类型选择为【IPsec VPN】，选择运营商，当前支持电信、联通、移动和外网CAP。

5. 完成参数设置后，单击【创建】。创建成功的VPN网关系统会分配一个公网IP，例如 203.195.147.82 。

步骤2：创建对端网关

在 VPN 通道创建前，需要创建对端网关：

1. 登录云平台，选择【云产品】>【计算与网络】>【私有网络(VPC)】进入私有网络控制台。
2. 在左侧目录中单击【VPN 连接】>【对端网关】，进入【对端网关】界面。
3. 选择地域，如示例中的广州，单击【新建】。

4. 填写对端网关名称（如：TomVPNUserGw）和 IDC 的 VPN 网关的公网 IP ，如： 202.108.22.5 。

5. 单击【创建】即可。

步骤3：创建 VPN 通道

1. 登录云平台，选择【云产品】>【计算与网络】>【私有网络(VPC)】进入私有网络控制台。
2. 在左侧目录中单击【VPN连接】>【VPN通道】，进入【VPN通道】界面。
3. 选择对应的地域和私有网络，如示例中的广州和 TomVPC ，单击【+新建】。

4. 输入通道名称（如：TomVPNConn），选择 VPN 网关 TomVPNGw 与对端网关 TomVPNUserGw ，并输入预共享密钥（如： 123456 ），单击【下一步: SPD策略】。

5. 输入 SPD 策略来限制本段哪些网段和对端哪些网段通信，在本例中本端网段即为子网 A 的网段 192.168.1.0/24 ，对端网段为 10.0.1.0/24 ，单击【下一步: IKE配置】。

6. （可选）配置 IKE 参数，如果不需要高级配置，可直接单击【下一步: IPsec配置】。

7. （可选）配置 IPsec 参数，如果不需要配置，可直接单击【下一步: 完成配置】。

8. 创建成功后，返回 VPN 通道列表页，单击【下载配置文件】并完成下载。

步骤4：本地网关配置

完成前3步后，云上 VPN 网关和 VPN 通道的配置已经完成，需要继续在“本地网关”上配置另一侧的 VPN 通道信息。本地网关一般会有以下部署场景：

- 打通云平台和本地数据中心
  本地网关是具有 VPN 功能的网络设备，一般为数据中心出口路由器或防火墙，您可在此网络设备上进行 VPN 配置，以完成“本地网关”配置。

  > 说明：由于网络设备生产厂商的不同（如 H3C、思科等），配置可能会有差异，请根据网络设备的实际情况进行配置。

- 打通不同云平台
  本地网关是您另一侧云平台 VPC 内部署的另一个 VPN 网关，您可以在另一个 VPN 网关上重复 步骤1 - 3，以完成“本地网关”的相关配置。

- 打通云平台和其他公有云
  本地网关是您目标公有云上的 VPN 网关，您需要在目标公有云上的 VPN 网关进行操作，以完成“本地网关”的 VPN 配置，具体配置方法请参考目标公有云的文档介绍。

> 注意：
>
> - 以上三种方式均要求您“本地网关”上的 VPN 配置，与 步骤3 中的 VPN 通道的信息一致，否则 VPN 隧道无法正常连通。
> - 云平台上 VPN 通道的配置信息可以通过控制台查看，您也可以通过下载配置文件并加载到本地数据中心的 IPsec VPN 网关中，完成配置。

步骤5：配置路由表

截止至步骤 4，我们已经将一条 VPN 通道配置成功，但仍需配置路由表，将子网 A 中的流量路由至 VPN 网关上，子网 A 中的网段才能与 IDC 中的网段通信。

1. 登录【私有网络(VPC)】控制台。
2. 在左侧目录中单击【子网】，选择对应的地域和私有网络，如示例中的广州和 TomVPC ，单击子网 A 所关联的路由表 ID，进入详情页。

3. 单击【+新增路由策略】。

4. 在弹出框中，输入目的端网段（ 10.0.1.0/24 ），下一跳类型选择【VPN 网关】，下一跳选择刚创建的 VPN 网关 TomVPNGw ，单击【确定】即可。

> 说明：若您的本地网关是另一侧云平台 VPC 内部署的 VPN 网关，请重复上述步骤，为本地网关配置路由。

步骤6：激活 VPN 隧道

1. 用 VPC 内的云服务器 ping 对端网段中的 IP， 以激活 VPN 隧道。
   例如： TomVPC 内的子网 A 中的云服务器 ping 10.0.1.1 。

创建SSL VPN连接

操作场景

通过 SSL VPN 连接，实现到私有网络的远程访问。

操作步骤

步骤一：创建SSL VPN网关

1. 登录云平台，选择云产品 > 云计算与网络 > **私有网络(VPC)**进入私有网络控制台。
2. 在左侧目录中单击 VPN 连接 > VPN 网关，进入 VPN 网关管理界面。
3. 选择地域，如示例中的广州，单击新建。

   > 说明：
   >
   > 若【新建】显示灰色，且鼠标移至上方时显示"无可用私有网络"，请 创建私有网络 后再进行新建 VPN 网关。

4. 填写 VPN 网关名称（如 TomVPNGw），选择所属网络（如示例中的 TomVPC）、带宽上限，VPN类型选择 SSL VPN，单击创建即可。VPN 网关创建完成后，系统随机分配公网 IP，如： 203.195.147.82 。

步骤二：创建SSL服务端

1. 单击 SSL 服务端，进入SSL服务端界面。
2. 单击新建，在弹出的新建SSL服务端对话框中配置参数，并单击创建。
   参数说明：
   - 所属网络：选择创建VPN连接的私有网络。
   - VPN网关：选择步骤4中创建的SSL VPN网关。
   - 本端网段：填写服务端本端网段，该网段必须属于私有网络CIDR范围内。
   - 客户端网段：填写客户端网段，仅支持10、172、192私有地址段，掩码范围为16-24，且不能与VPC网段重叠。
   - SSL连接数：选择SSL连接数。
   - 协议、端口、加密算法、认证算法、是否压缩参数取值如图所示，暂不支持修改。

SSL服务端列表：

步骤三：创建SSL客户端

1. 单击 SSL 客户端，进入SSL客户端界面。
2. 单击新建，在弹出的新建 SSL 客户端对话框中填写SSL客户端名称，选择步骤6中创建的SSL服务端，并单击创建。

SSL客户端列表：

3. 单击下载配置，证书用于与服务端验证身份。

> 说明：
>
> 用户使用证书和密钥与VPN网关建连，用户侧验证服务端证书，服务端验证用户端证书，校验通过后，服务端从客户端IP地址池中分配一个IP给用户，该IP用于和VPC内VM通信时使用。

步骤四：配置路由

1. 在VPC内配置路由转发策略，目的地址为客户端IP地址池，下一跳到SSL VPN网关。

功能验证

在客户端浏览器访问私有网络内服务，如能正常访问，说明配置正确，如访问异常，请检查并记录配置信息，及时联系技术支持人员。

操作指南
操作总览

该章节提供VPN控制台使用指南，通过VPN控制台可创建并管理VPN相关操作。在您使用VPN连接时，可参考本章节，了解VPN网关创建、控制台相关功能及操作指导。

- 如果您需要创建IPsec VPN连接，可参考VPN网关、对端网关、VPN通道的操作指导。
- 如果您需要创建SSL VPN连接，可参考VPN网关、SSL服务端、SSL客户端的操作指导。

常用操作

- 查看监控数据
- 设置告警
- 修改 VPN 通道配置

查看监控数据

VPN 通道和 VPN 网关提供监控数据查看功能。

VPN 网关

1. 登录【私有网络(VPC)】控制台。
2. 单击左导航栏中【VPN连接】>【VPN网关】。
3. 选择地域和私有网络，单击列表中需要查看的 VPN 网关监控图标，即可查看监控数据。

VPN 通道

1. 登录【私有网络(VPC)】控制台。
2. 单击左导航栏中【VPN 连接】>【VPN 通道】。
3. 选择地域和私有网络，单击列表中需要查看的 VPN 通道监控图标，即可查看监控数据。

设置告警

VPN 通道提供告警功能：

1. 登录云平台，选择【云产品】>【管理与审计】>【云监控】，进入【云监控】界面。
2. 在左侧目录选择【告警配置】>【告警策略】，进入告警策略配置页面，单击【新增】。
3. 填写告警策略名称，策略类型选择【私有网络】>【VPN通道】，选择告警对象，设置告警策略，选择告警接收组和告警渠道，单击【完成】，即可在告警策略列表中查看已设置的告警策略。

4. 查看告警信息
   告警条件被触发后，您将通过已选择的告警渠道接收到告警通知（短信 / 邮件 / 站内信等），也可以单击左侧目录【告警历史】查看。

修改 VPN 通道配置

1. 登录【私有网络(VPC)】控制台。
2. 在左侧目录中单击【VPN 连接】>【VPN 通道】，进入管理页。
3. 单击需要修改的 VPN 通道 ID，进入详情页。
4. 在基本信息页中修改基本信息和 SPD 策略。

5. 单击【高级配置】选项卡，可在高级配置中修改 IKE 和 IPsec 配置。

VPN网关

创建VPN网关

操作场景

VPN网关是VPN连接的重要组成部分，该章节主要介绍如何通过控制台创建VPN网关。

操作步骤

1. 登录 私有网络VPC 控制台，在左侧导航列选择 VPN 连接 > VPN网关，进入VPN网关控管理界面。
2. 单击新建，系统弹出新建 VPN 网关对话框。
3. 根据网关类型，设置相关参数。
    - IPsec VPN

    - SSL VPN

参数含义：

- 网关名称：自定义网关名称。
- 所属网络：选择VPN网关所属私有网络。
- 带宽上限：系统支持5M、10M、20M、50M、100M规格的带宽，请按需选择。
- VPN类型：选择IPsec VPN或SSL VPN。
- 运营商：仅当 VPN 类型为 IPsec VPN 时才展示该参数，当前支持电信、联通、移动和外网CAP，请按需选择。

4. 完成网关参数设置后，单击创建启动创建任务，当状态列显示为运行中中，创建成功。

查询VPN网关

操作场景

VPN网关管理界面展示所有已创建的VPN网关，进入具体网关可查看网关详情及监控信息，同时系统支持通过VPN网关名称或ID进行快速检索。

操作步骤

1. 进入 VPN 网关管理界面，可查询到所有VPN网关信息，一个网关实例为一条。

2. 单击网关ID，可进入基本信息界面，查询网关详情及路由策略信息。

3. 单击监控页签，界面将展示网关的指标信息，指标包括外网出带宽、外网入带宽、出包量、入包量。也可通过VPN网关界面的进入指标展示界面。
   字段说明：

- 实时：可查看当前时刻的指标数据。
- 近24小时：可查看近24小时的指标数据。
- 近7天：可查看近7天的指标数据。
- 选择日期：可自定义查询指定时间段的指标数据。
- 数据对比：可查看某两个时刻的实时数据比对详情。

- ：可变换指标的展示方式。

5. 单击右上方的，可设置界面展示参数。

6. 在右上方的搜索框中输入VPN网关名称或ID，可快速搜索网关实例。

删除VPN网关

操作场景
可删除未建立连接的VPN网关实例，处于准备中或已经建立VPN连接的网关实例不能删除。
操作步骤

1. 在 VPN 网关管理界面，单击需要删除的网关实例右侧的删除。
2. 在弹出的确认对话框中，单击确定即可完成删除操作。

VPN通道

创建 VPN 通道

1. 登录云平台，选择【云产品】>【计算与网络】>【私有网络(VPC)】进入私有网络控制台。
2. 在左侧目录中单击【VPN连接】>【VPN通道】，进入【VPN通道】界面。
3. 选择对应的地域和私有网络，如示例中的广州和TomVPC，单击【+新建】。

4. 输入通道名称（如：TomVPNConn），选择 VPN 网关TomVPNGw与对端网关TomVPNUserGw，并输入预共享密钥（如：123456），单击【下一步: SPD策略】。

5. 输入 SPD 策略来限制本段哪些网段和对端哪些网段通信，在本例中本端网段即为子网 A 的网段192.168.1.0/24，对端网段为10.0.1.0/24，单击【下一步: IKE配置】。

6. （可选）配置 IKE 参数，如果不需要高级配置，可直接单击【下一步: IPsec配置】。

7. （可选）配置 IPsec 参数，如果不需要配置，可直接单击【下一步: 完成配置】。
   创建成功后，返回 VPN 通道列表页，单击【下载配置文件】并完成下载。

8. 创建成功后，返回 VPN 通道列表页，单击【下载配置文件】并完成下载。

查询 VPN 通道

VPN 通道管理界面展示所有已创建的 VPN 通道，进入具体通道可查看网关详情及监控信息，同时系统支持通过 VPN 通道名称或 ID 进行快速检索。

1. 进入【VPN 通道】管理界面。
   通道列表展示了所有 VPN 通道信息，一个通道实例为一条。
2. 在通道列表右上角，通过搜索框查询 VPN 通道。
3. （可选）可单击搜索框旁的展示列设置，设置需要展示的通道参数信息。

4. 单击通道 ID，可进入【基本信息】界面，查询通道详情信息。

5. 单击【监控】页签，界面将展示网通道的指标信息，指标包括外网出带宽、外网入带宽、出包量、入包量。也可通过 VPN 通道界面的  进入指标展示界面。

删除 VPN 通道

对于不再使用的 VPN 通道，您可以在通道列表中删除。

1. 进入【VPN 通道】管理界面。
2. 在通道列表找到待删除的 VPN 通道，然后在操作列单击【删除】。
3. 在确认删除对框中单击【确定】。

对端网关

创建对端网关

在 VPN 通道创建前，需要创建对端网关：

1. 登录云平台，选择【云产品】>【计算与网络】>【私有网络(VPC)】进入私有网络控制台。
2. 在左侧目录中单击【VPN 连接】>【对端网关】，进入【对端网关】界面。
3. 选择地域，如示例中的广州，单击【新建】。

4. 填写对端网关名称（如：TomVPNUserGw）和 IDC 的 VPN 网关的公网 IP ，如：202.108.22.5。

5. 单击【创建】即可。

查询对端网关

支持通过对端网关名称或 ID 进行快速检索。

1. 进入【对端网关】管理界面。
   通道列表展示了所有对端网关信息。

2. 在通道列表右上角，通过搜索框查询对端网关。
3. （可选）可单击搜索框旁的展示列设置，设置需要展示的对端网关参数信息。
4. 单击对端网关 ID，可进入【基本信息】界面，查询对端网关详情信息。

删除对端网关

对于不再使用的对端网关，您可以在对端网关列表中删除。

1. 进入【对端网关】管理界面。
2. 在通道列表找到待删除的对端网关，然后在操作列单击【删除】。
3. 在确认删除对框中单击【确定】。

SSL服务端

创建 SSL 服务端

1. 单击 SSL 服务端，进入SSL服务端界面。
2. 单击新建，在弹出的新建 SSL 服务端对话框中配置参数，并单击创建。

参数说明：

- 所属网络：选择创建 VPN 连接的私有网络。
- VPN网关：选择步骤4中创建的 SSL VPN 网关。
- 本端网段：填写服务端本端网段，该网段必须属于私有网络 CIDR 范围内。
- 客户端网段：填写客户端网段，仅支持10、172、192私有地址段，掩码范围为16-24，且不能与 VPC 网段重叠。
- SSL 连接数：选择 SSL 连接数。
- 协议、端口、加密算法、认证算法、是否压缩参数取值如图所示，暂不支持修改。
  SSL 服务端列表：

查询 SSL 服务端

支持通过对 SSL 服务端名称或 ID 进行快速检索。

1. 进入 SSL 服务端管理界面。
   通道列表展示了所有 SSL 服务端信息。
2. 在 SSL 服务端列表右上角，通过搜索框查询 SSL 服务端。
3. （可选）可单击搜索框旁的展示列设置，设置需要展示的 SSL 服务端参数信息。
4. 单击对 SSL 服务端 ID，可进入基本信息界面，查询 SSL 服务端详情信息。

删除 SSL 服务端

对于不再使用的 SSL 服务端，您可以在列表中删除。

1. 进入 SSL 服务端管理界面。

2. 在 SSL 服务端列表找到待删除的 SSL 服务端，然后在操作列单击删除。
3. 在确认删除对框中单击确定。

SSL客户端

创建 SSL 客户端

1. 单击【SSL 客户端】，进入 SSL 客户端界面。
2. 单击【新建】，在弹出的【新建 SSL 客户端】对话框中填写 SSL 客户端名称，选择步骤6中创建的 SSL 服务端，并单击【创建】。

   SSL 客户端列表：

3. 单击【下载配置】，证书用于与服务端验证身份。
   用户使用证书和密钥与 VPN 网关建连，用户侧验证服务端证书，服务端验证用户端证书，校验通过后，服务端从客户端 IP 地址池中分配一个 IP 给用户，该 IP 用于和 VPC 内VM通信时使用。

查询 SSL 客户端

支持通过对 SSL 客户端名称或 ID 进行快速检索。

1. 进入【 SSL 客户端】管理界面。
   通道列表展示了所有 SSL 客户端信息。
2. 在 SSL 客户端列表右上角，通过搜索框查询 SSL 客户端。
3. （可选）可单击搜索框旁的展示列设置，设置需要展示的 SSL 客户端参数信息。
4. 单击对 SSL 客户端 ID，可进入【基本信息】界面，查询 SSL 客户端详情信息。

删除 SSL 客户端

对于不再使用的 SSL 客户端，您可以在列表中删除。

1. 进入【SSL 客户端】管理界面。
2. 在SSL 客户端列表找到待删除的SSL 客户端，然后在操作列单击【删除】。
3. 在确认删除对框中单击【确定】。

常见问题

概念类

什么是 VPN 连接？

VPN 连接是一种通过公网加密通道连接用户的对端 IDC 和私有网络的方式。详情请参见 产品概述。

什么是 VPN 通道？

VPN 网关和对端网关建立后，即可建立 VPN 通道，用于私有网络和外部 IDC 之间的加密通信，详情请参见 产品概述。

什么是 VPN 网关？

VPN 网关是私有网络建立 VPN 连接的出口网关，与对端网关（IDC 侧的 IPsec VPN 服务网关）配合使用，主要用于云平台私有网络和外部 IDC 之间建立安全可靠的加密网络通信。云平台 VPN 网关通过软件虚拟化实现，采用双机热备的策略，单台故障时自动切换，不会影响业务正常运行。

VPN 网关根据带宽上限分为8种设置，分别为：5M、10M、20M、50M、100M。

什么是 IPsec VPN？

IPsec VPN 是一种通过公网加密通道连接用户的 IDC 和私有网络的方式。云平台私有网络 IPsec VPN 接入分为以下几个组成部分：

- VPN 网关：VPN 网关是私有网络的 IPsec VPN 网关，与对端网关（用户 IDC 侧的 IPsec VPN 服务网关）配合使用，主要用于私有网络和用户的 IDC 之间建立安全可靠的加密网络通信对端网关。
- 对端网关：对端网关指用户 IDC 机房的 IPsec VPN 服务网关在私有网络内的映射，对端网关需与 VPN 网关配合使用，一个 VPN 网关可与多个对端网关建立带有加密的 VPN 网络通道。
- VPN 通道：加密的公网 IPsec VPN 通道，在 VPN 网关和对端网关建立后，即可以建立 VPN 通道，用于私有网络和用户的 IDC 之间的加密通信。

使用 VPN 有什么约束？

使用 VPN 时，您需要注意 VPN 连接和对端网关 IP 地址上的约束，详情请参见 使用约束。

可以创建多少个 VPN 网关、VPN 通道？

不同的资源有不同的创建数量限制，详情请参见 VPC 内的资源配额详情 ，如需更高配额，请填写 工单申请 。

一个 VPC 可以通过 VPN 连接与多个 IDC 互联吗？

可以，目前私有网络可以建立 VPN 网关并在每个 VPN 网关上建立多个 VPN 通道，每个 VPN 通道可以打通一个本地 IDC。

两个 VPC 之间通信可以通过 VPN 连接实现吗？

可以，用户需要分别在两个 VPC 内购买 VPN 网关、配置 VPN 通道和对端网关，但配置较为复杂。VPC互联可使用对等连接。

通过 VPN 连接的私有网络和 IDC 之间的网络质量如何保证？

- VPN 连接在私有网络与 IDC 之间是通过公网传输的，故整体网络质量依赖公网网络的质量，当公网网络出现时延、丢包、抖动时，VPN 连接也会相应受到影响，如果您需要更加稳定的通信质量，建议使用 专线接入 服务。
- 云平台会为您的 VPN 网关提供24小时监控，对异常情况进行告警，紧急情况下还会有运维人员会介入处理。用户也可以在控制台实时监控 VPN 网关和通道的流量状态，如果发现异常，请及时 联系我们。

专线接入与 IPSec VPN 连接有什么区别？

- IPsec VPN 连接利用公网和 IPsec 协议在用户的数据中心和私有网络之间建立加密的网络连接。VPN 网关的购买、生效和配置可以在几分钟内完成。但是 VPN 连接可能会受到 Internet 抖动、阻塞等公网质量而中断，当用户的业务对网络连接质量要求不高时，是一种快速部署高性价比选择。
- 专线接入则提供了一个用户专用的网络连接方案，施工时间较长，但可以提供高质量高可靠的网络连接服务，当用户的业务对网络质量和网络安全要求较高时，可以选择此方案进行部署。

两者的具体区别如下表：

优势	专线接入	IPsec VPN
稳定的网络延时	专线接入网络延时可靠有保证，接入网络基于专用线路，用户可以通过固定的路由配置免去拥堵或故障绕行带来的时延不稳定困扰。	IPsec VPN 接入网络连接基于 Internet，可能由于网络高峰链路阻塞导致路由绕行，时延不稳定。
高可靠的容灾接入	专线接入的接入设备及网络转发设备均采用分布式集群化部署，全链路高可靠配置，支持带保护的双线接入，满足用户高于99.95%可用性的苛刻要求。	IPsec VPN 网关采用双机热备份配置，具备网关层高可靠，但由于 Internet 网络链路不可靠，无法提供专线级网络可靠保证。
支持大带宽	专线接入单线路最大支持10Gbps带宽连接，还可以接入多条10Gbps链路做网络负载均衡，无理论上限。	IPsec VPN 单网关最大支持100Mbps带宽上限，私有网络支持多 VPN 网关配置，可以通过多 VPN 网关的配置满足大于100Mbps的 VPN 接入。
安全性高	专线接入网络链路用户独占，无数据泄露风险，安全性高，满足金融、政企等高等级网络连接要求。	IPsec VPN 网络传输基于 IKE 协议的预共享密钥的加密，可以满足绝大多数网络传输安全性要求。
支持网络地址转换	专线接入支持在网关上配置网络地址转换服务，支持专线两端的 IP 映射和私有网络端的 IP 端口映射，完美搞定多第三方的网络互联时的地址冲突难题。	暂不支持。

为什么 VPN 通道已连接，但是两端没有流量或无法 Ping 通？

请您依次排查 SPD 策略（感兴趣流）、路由表、安全组是否配置合理：

1. 排查两端的 SPD 策略配置
   请检查 VPN 通道两侧的感兴趣流设置是否合理，如果您 VPN 的流量经过了 NAT 设备，请防止访问云平台的流量被 NAT 匹配而未走到 VPN 通道，造成无可用激活流量而无法激活 VPN 通道的问题。

2. 排查两端的路由配置
   请确保路由表中已经创建了去往您对端内网的路由策略，并将该路由指向了 VPN 网关。

3. 排查两端安全策略配置

   - CVM 的安全组出站策略允许主动访问对端网段，安全组入站策略允许对端网段主动访问您的 CVM。
   - 您对端的 VPN 网关安全策略已开放了您的内网服务器与云 CVM 之间互访权限。
   - 检查您对端的内网服务器与 VPN 设备之间是否存在安全限制。
   - 检查 VPC 的子网是否绑定了网络 ACL，若绑定需开放相应访问网段。

如果检查结束后仍无法解决您的问题，请 提交工单 与我们联系。

是否可以通过 VPN 连接访问 Internet？

不可以。云平台 VPN 连接产品在国家相关政策法规下提供服务，VPN 网关仅提供接入 VPC 的功能，不提供访问 Internet 功能。

功能类

VPN 网关是如何实现的，可用性如何？

- VPN 网关是通过网络功能虚拟化（NFV）实现的，采用双机热备的策略，单台故障时自动切换，不会影响业务正常运行。
- VPN 通道在公网中运行，公网网络出现阻塞、抖动、延迟等问题都会对 VPN 网络质量产生影响。如果业务对网络传输的延迟、抖动容忍度较低，建议使用 专线接入。

VPN 通道未连通如何处理？

VPN 通道连通的配置过程需要两端协商信息一致才可成功建立连接，需要依次检查两端配置的一致性，推荐的检查思路如下：

> 注意：
>
> - 任何一个参数不一致，VPN 通道都无法建立。
> - 不同厂家设备、云平台服务提供商的默认 VPN 配置不尽相同。

1. 检查第一阶段 IKE 配置信息。
   请您检查第一阶段所需的 IKE 版本号、身份证认证方法、加密算法、认证算法、协商模式、两端标识、DH group、IKE sa lifetime 两端的所有参数是否保持一致，如果有不一致的请修改一致后再尝试。
   TCloudFinanceZone VPN 网关的第一阶段协商参数的默认配置为：

IKE 配置项	默认配置	其他可选配置
IKE	IKEv1	-
身份证方法	预共享密钥	-
加密算法	3DES	AES-128， AES-192， AES-256，DES
认证算法	MD5	SHA1
协商模式	main	aggressive
本端标识	IP Address（默认为云平台侧 VPN 网关的公网 IP 地址）	FQDN
对端标识	IP Address（默认对端 VPN 网关的公网 IP 地址）	FQDN

IKE 配置项	默认配置	其他可选配置
DH group	DH1	DH2，DH5，DH14，DH24
IKE SA Lifetime	86400s	支持自定义
2. 检查第二阶段 IPsec 配置信息		
请您检查第二阶段的所需的加密算法、认证方法、报文封装模式、安全协议、PFS、IPsec SA 生成周期两端的所有参数是否一致，如果有不一致的请修改一致后再尝试。		
TCloudFinanceZone VPN 网关的第二阶段 IPsec 参数的默认配置为：		

IPsec 配置项	默认配置	其他可选配置
加密算法	AES-128	AES-128，AES-192，AES-256，DES
认证算法	MD5	SHA1
报文封装模式	Tunnel	-
安全协议	ESP	-
PFS	disable	dh-group1、dh-group2、dh-group5、dh-group14、dh-group24
IPsec sa Lifetime	3600s	支持自定义
IPsec sa Lifetime	1843200KB	支持自定义

为什么 VPN 网关与 VPN 通道显示的监控数据有时不一致？

目前 VPN 网关与 VPN 通道的数据采集位置与上报间隔存在区别，其中 VPN 网关的统计粒度为1分钟，VPN 通道的统计粒度为10秒，统计粒度不一致。因此在监控页进行数据聚合的时候，会造成 VPN 网关与 VPN 通道的展示数据不一致的情况。

如何配置 VPN？

IPsec VPN 可以在控制台实现全自助配置，详情请参见 快速入门。

如何创建 VPN 网关？

用户可以进入【私有网络(VPC)】控制台创建 VPN 网关，详情请参见 创建 VPN 网关。

如何创建 VPN 通道？

用户可以进入【私有网络(VPC)】控制台创建 VPN 通道，详情请参见 创建 VPN 通道。

如何查看 VPN 连接监控数据？

用户可以进入【私有网络(VPC)】控制台查看 VPN 连接监控数据，详情请参见 查看监控数据。

如何设置 VPN 连接告警？

用户可以进入【私有网络(VPC)】控制台设置 VPN 连接告警，详情请参见 设置告警。

如何修改 VPN 通道配置？

用户可以进入 【私有网络(VPC)】控制台修改 VPN 通道配置，详情请参见 修改 VPN 通道配置。

词汇表

对端网关

对端网关指您 IDC 机房的 IPsec VPN 服务网关在私有网络内的映射，对端网关需与 VPN 网关配合使用，一个 VPN 网关可与多个对端网关建立带有加密的 VPN 网络通道。

IPsec VPN

IPsec VPN（Internet Protocol Security VPN）是一种通过公网加密通道连接您的 IDC 和私有网络的方式。

路由表

路由表（Routing Table）包含一系列路由策略，用于定义私有网络内每个子网的网络流量走向。每个子网有且只有一个关联路由表，每个路由表可以关联同一个私有网络中的多个子网。

路由策略

路由策略（Routing Policy）是网络流量所经过的途径规则，每条路由策略包含了三个参数：

1. 目的端：目的网段描述，目的端不可以为路由表所在私有网络内的 IP 段。
2. 下一跳类型：私有网络下一跳类型支持“公网网关”、“VPN 网关”、“专线网关”等一系列的类型，您需要先创建此类网关，否则无法拉取到此下一跳类型。
3. 下一跳：指定关联到该路由表的子网流量具体跳转至哪个下一跳网关。

私有网络

私有网络（Virtual Private Cloud）在云平台构建出独立的网络空间，与您在数据中心运行的传统网络极其相似，但是托管在云平台私有网络内的是您在云平台上的服务资源，包括：云服务器、负载均衡、云数据库 等云服务资源。您完全不用关心网络设备的采购和运维，而是通过软件自定义网段划分、IP 地址、路由策略等。您不仅可以通过 弹性 IP、NAT 网关 和 公网网关 等灵活访问 Internet，您也可以通过 VPN / 专线接入 将私有网络与您的数据中心连通。同时，云平台私有网络的 对等连接 服务可以帮助您轻松实现全球同服和两地三中心容灾。另外，云平台私有网络中的 安全组 和 网络 ACL 可以多维度、全方位的满足您的网络安全需求。

VPN 网关

VPN 网关 是私有网络的 IPsec VPN 网关，与对端网关（您 IDC 侧的 IPsec VPN 服务网关）配合使用，主要用于私有网络和您的 IDC 之间建立安全可靠的加密网络通信对端网关。

VPN 通道

VPN 通道 指加密的公网 IPsec VPN 通道，VPN 网关和对端网关建立后，可以建立 VPN 通道，用于私有网络和您的 IDC 之间的加密通信。

物理专线

物理专线是连接云平台与本地数据中心的物理线路连接，一个物理专线可以与多个地域的专线网关建立专用通道。

子网

子网（Subnet）是对私有网络网段的灵活划分，可以在不同子网内部署应用程序和服务，安全灵活地在云平台 VPC 中托管多层 Web 应用程序。

专线接入

专线接入（Direct Connect）是一种快速连接TCloudFinanceZone与本地数据中心的方法，您可以通过一条物理专线一次性打通位于多地域的TCloudFinanceZone计算资源，实现灵活可靠的混合云部署。专线接入支持无单点的双线热备接入方式，满足金融等高网络互联要求。

专用通道

专用通道是物理专线的网络链路划分，可以创建连接至不同专线网关的专用通道实现本地数据中心与多个私有网络的互联。

专线网关

专线网关是私有网络的专线流量入口，可以接入多个专用通道与多个本地数据中心互联。