VPN连接

产品文档

文档目录

产品简介
VPN 网关

最近更新时间: 2023-03-20 15:18:06

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，主要用于私有网络和外部 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实现，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网关根据带宽上限分为 5 种设置，分别为:5M、10M、20M、50M、100M。您可以随时调整VPN 网关带宽设置，即时生效。

对端网关

最近更新时间: 2023-03-20 15:18:06

对端网关是指 IDC 机房的 IPsec VPN 服务网关，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

最近更新时间: 2023-03-20 15:18:06

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。当前 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、抖动会对 VPN 网络质量有影响。如果业务对延时、抖动敏感，建议通过专线接入私有网络。
云平台上的VPN通道在实现IPsec中使用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。
私有网络内可以建立 VPN 网关，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。需要注意的是，在建立 VPN 连接之后，您需要在路由表中配置相关路由策略，才能真正实现通信。

产品优势

最近更新时间: 2023-03-20 14:21:08

- **安全**

采用IKE和IPsec对传输的数据进行加密，在internet上建立一条安全、可信的数据隧道，保障所传输数据的安全

- **高可用**

采用双机热备架构，实现故障秒级切换且无需重建通道，保障通信会话不中断、上层应用无感知

- **可视化管理**

通过图表直观展现VPN性能状态，支持流量管控功能，通过多维度监控对故障设定预警，及时定位和解决问题

- **操作简单**

云端配置实时生效，本地网关自动生成配置文件，导入设备即可完成配置

- **服务集成**

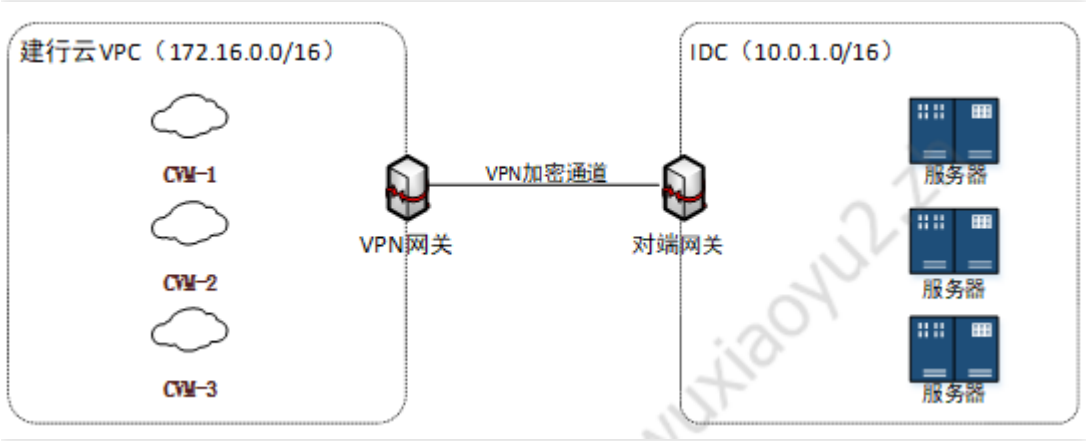
可与专线接入、私有网络等建行云其他服务集成，搭配不同的产品构筑端到端云上解决方案

应用场景

私有网络与 IDC 通信

最近更新时间: 2023-03-20 15:18:06

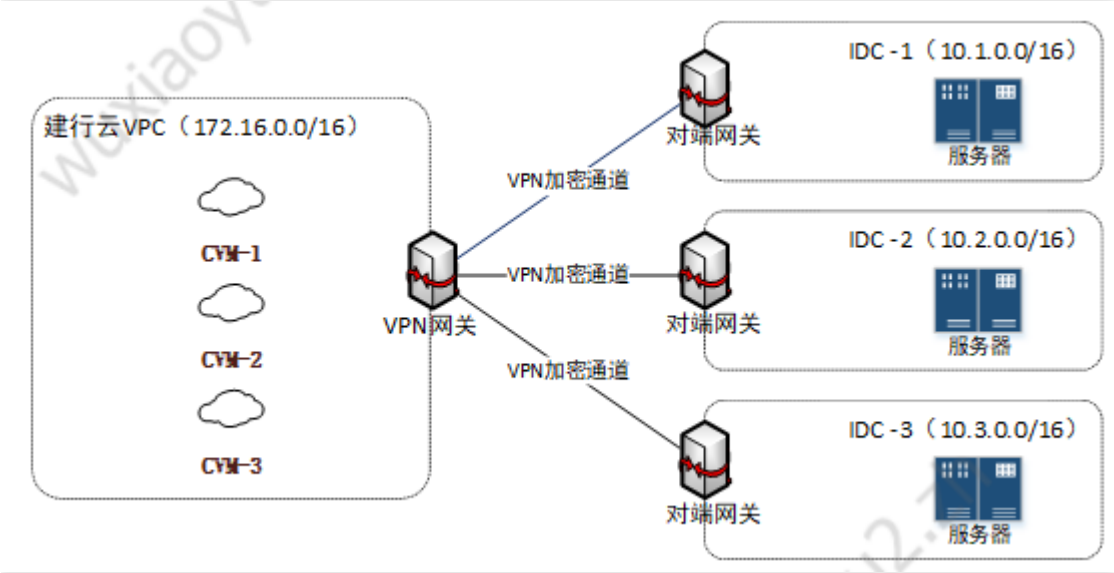
VPN连接实现私有网络（VPC）与IDC的互访通信。



单个私有网络通过多条VPN通道分别 与 多个 IDC 通信

最近更新时间: 2023-03-20 15:18:06

该场景仅实现 IDC1 与 VPC 通信、IDC2 与 VPC 通信，IDC3 与 VPC 通信，而 IDC1、IDC2、IDC3 之间无需通信。
该场景建议使用 SPD 策略路由的方式，分别创建 VPC > IDC1、VPC > IDC2、VPC > IDC3 的规则即可。



快速入门
配置信息

最近更新时间: 2023-03-20 15:18:06

VPN 通道的建立包括以下配置信息:

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

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

1 基本信息

协议类型:IKE/IPsec

预共享秘钥:预共享密钥是用于验证 L2TP/IPSec 连接的 Unicode 字符串，本端和对端必须使用相同的预共享密钥。

2 SPD(Security Policy Database)策略

SPD(Security Policy Database)策略由一系列 SPD 规则组成，每条规则用于指定 VPC 内哪些网段可以和 IDC 中哪些网段通信。

每条 SPD 策略对应一个本端网段和多个对端网段，本段网段和对端网段不能重叠；

所有策略的集合中本端网段之间不可重叠； 每个本端网段的多条对端网段不可重叠；

对端网段不可与私有网络网段重叠

下面是一个正确的实例:

SPD 策略 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。

SPD 策略 2 本端网段 10.0.1.0/24，对端网段为 192.168.2.0/24。

SPD 策略 3 本端网段 10.0.2.0/24，对端网段为 192.168.2.0/24。

3 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，这样做的优点是快速建立连接，而代价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，因此两端拥有兼容的配置是至关重要的
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

4 Ipsec 信息

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-group1、dh-group2、dh-group5、dh-group14和dh-group24
IPsec SA lifetime(s)	单位：秒

配置项	说明
IPsec SA lifetime(KB)	单位：KB

使用引导

最近更新时间: 2023-03-20 15:18:06

VPN 连接约束

关于 VPN 连接，您需要注意的是:

- VPN连接稳定性依赖运营商公网质量，无法提供 SLA 服务协议保障。
- VPN中断后，需要手动重新拨入，不支持自动重新建链。
- 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，子网内云主机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 内云主机 ping 对端网段中的 IP 以激活此 VPN 通道；
- 地址段为58.*/119.*/223.*的VPN网关不支持运营商故障下的自动切换，可申请新的VPN网关（确认地址段为103.*）进行替换。；
- VPN 网关互联网带宽受限于整体互联网运行情况，极端情况下可能会出现拥塞；
- VPN 连接 SPD 或路由网段不可以指定为如下网段：

全0、全255或224开头的组播地址。

回环地址：127.x.x.x/8。

IPv6 网段。

对端网关 IP 地址约束

对端网关的公网IP不支持以下 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，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;
- IPv6网段

资源限制

资源	限制（个）
每个私有网络内 VPN 网关个数	10
同一地域内对端网关个数	20
同一个对端网关支持的VPN通道数	10

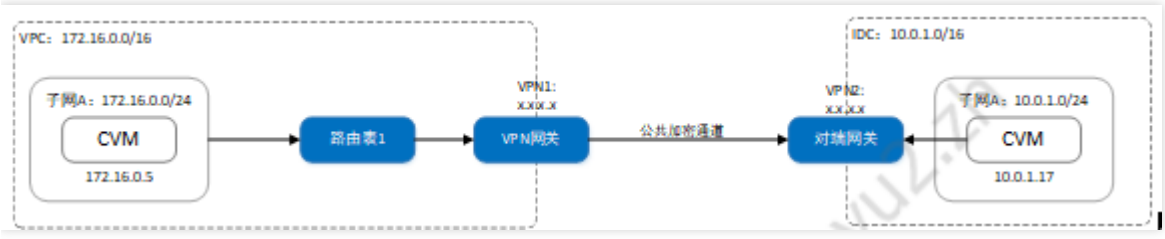
资源	限制（个）
同一VPN网关可创建的VPN通道数	20
每个 VPN 通道的 SPD 个数	10
每个 SPD 支持的对端网段数	50

接入引导

IPsec VPN 可以在控制台实现全自助配置，您需要完成以下几步才能实现使 VPN 连接生效:

1) 创建 VPN 网关
2) 创建对端网关
3) 创建 VPN 通道
4) 在自有 IPsec VPN 网关中加载配置文件
5) 设置路由表
6) VPN 通道激活

示例:
通过 IPsec VPN 连接打通您在武汉的私有网络 CCBVPC 中子网 A 172.16.0.0/24与您的 IDC 中子网 10.0.1.0/24，而您 IDC 中 VPN 网关的公网 IP 是X.X.X.X。



您需要完成以下几个步骤:
第一步:创建 VPN 网关

1) 登录云平台控制台，点击导航条【私有网络】，进入私有网络控制台；
2) 点击左导航栏中【VPN 连接】–【VPN 网关】选项卡；

3) 在列表的上端选择私有网络 CCBVPC 所在武汉和私有网络CCBVPC，点击【新建】；

4) 填写 VPN 网关名称(如: CCBVPNGw)选择合适的带宽配置，VPN 网关创建完成之后，系统随机分配公网 IP。

第二步:创建对端网关

在 VPN 通道创建前，需要创建对端网关:

1) 登录云平台控制台，点击导航条【私有网络】，进入私有网络控制台；

2) 点击左导航栏中【VPN 连接】–【对端网关】选项卡；

3) 在列表的上端选择地域:武汉，点击【新建】；

4) 填写对端网关名称(如: CCBVPNUserGw)和 IDC 的 VPN 网关的公网 IP；

5) 点击【创建】，即可在对端网关列表查看到新建的对端网关。

第三步:创建 VPN 通道

创建 VPN 通道分为以下几个步骤:

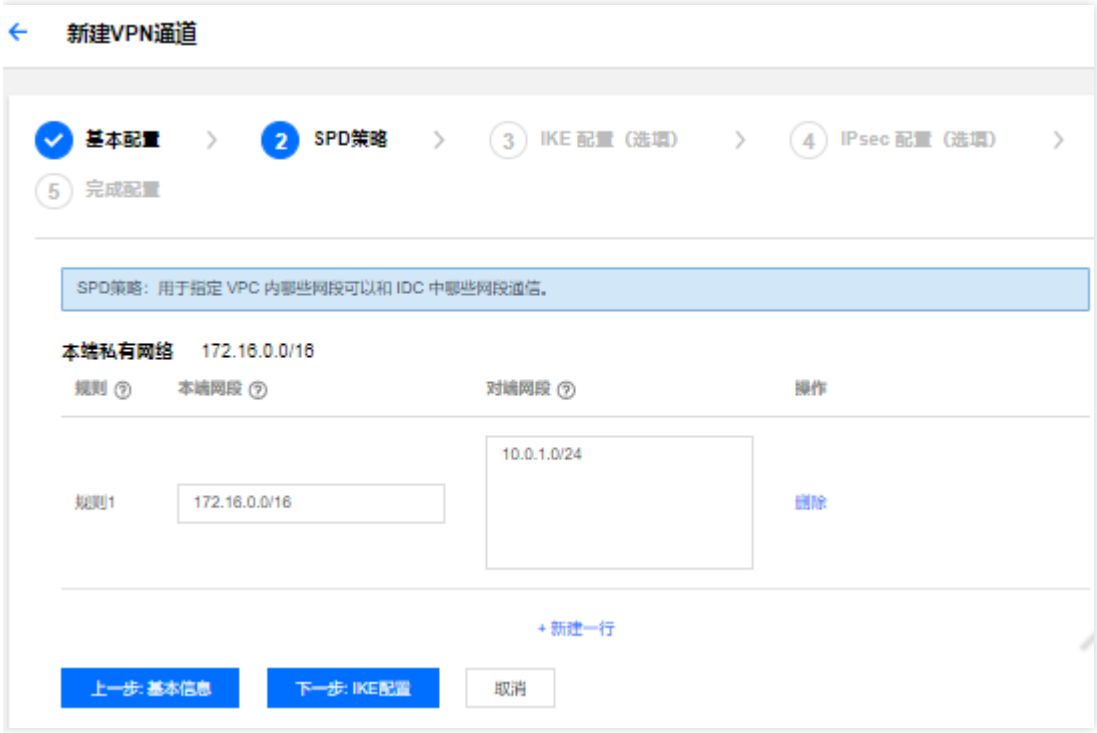
1) 登录云平台控制台，点击导航条【私有网络】，进入私有网络控制台；

2) 点击左导航栏中【VPN 连接】–【VPN 通道】选项卡；

3) 在列表的上端选择私有网络 CCBVPC 所在武汉和私有网络CCBVPC，点击【新建】；

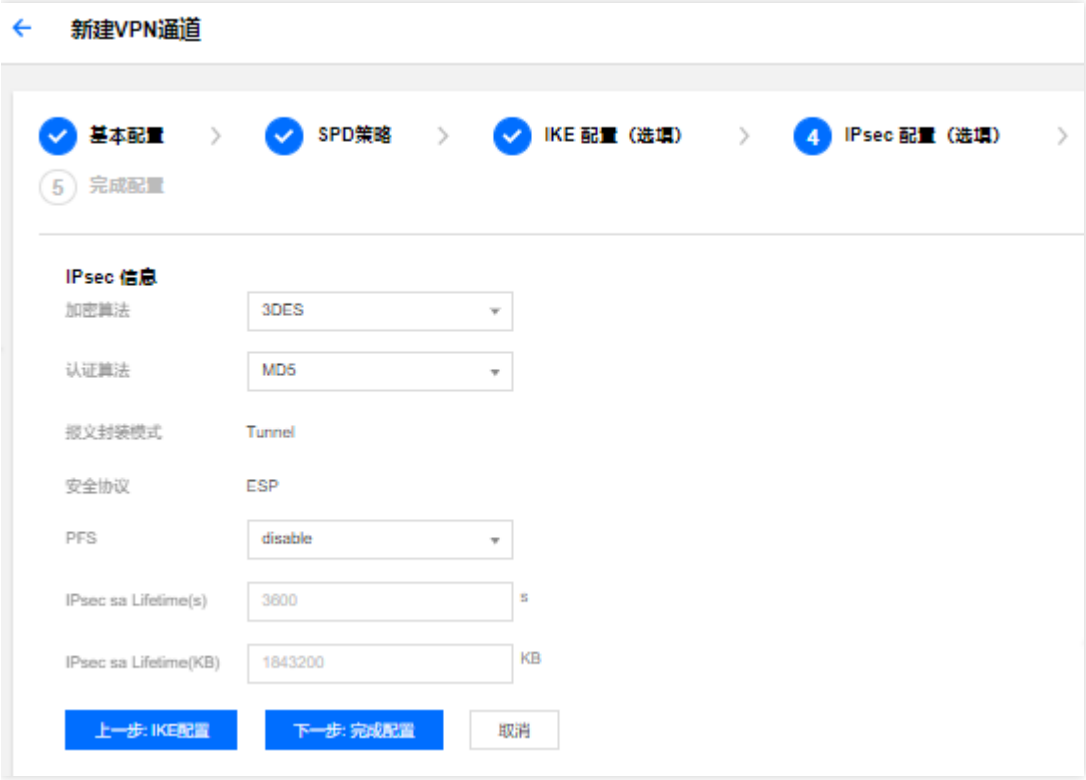
4) 输入通道名称(如: CCBVPNConn)，选择 VPN 网关CCBVPNGw与对端网关CCBVPNUserGw， 并输入预共享密钥(如:123456)；

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 172.16.0.0/24，对端网段为10.0.1.0/24，点击【下一步】；



6) (可选)第三步配置 IKE 参数(可选)，如果您不需要高级配置可直接点击【下一步】；

7) (可选)第四步配置 IPsec 参数(可选)，如果您不需要配置，可直接点击【完成配置】；



8) 点击完成 VPN 通道，下载配置文件。

第四步:在自有 IPsec VPN 网关中加载配置文件

将第三步生成的配置文件在您 IDC 的 IPsec VPN 网关中加载配置，才可实现 VPN 通道的网络互通。

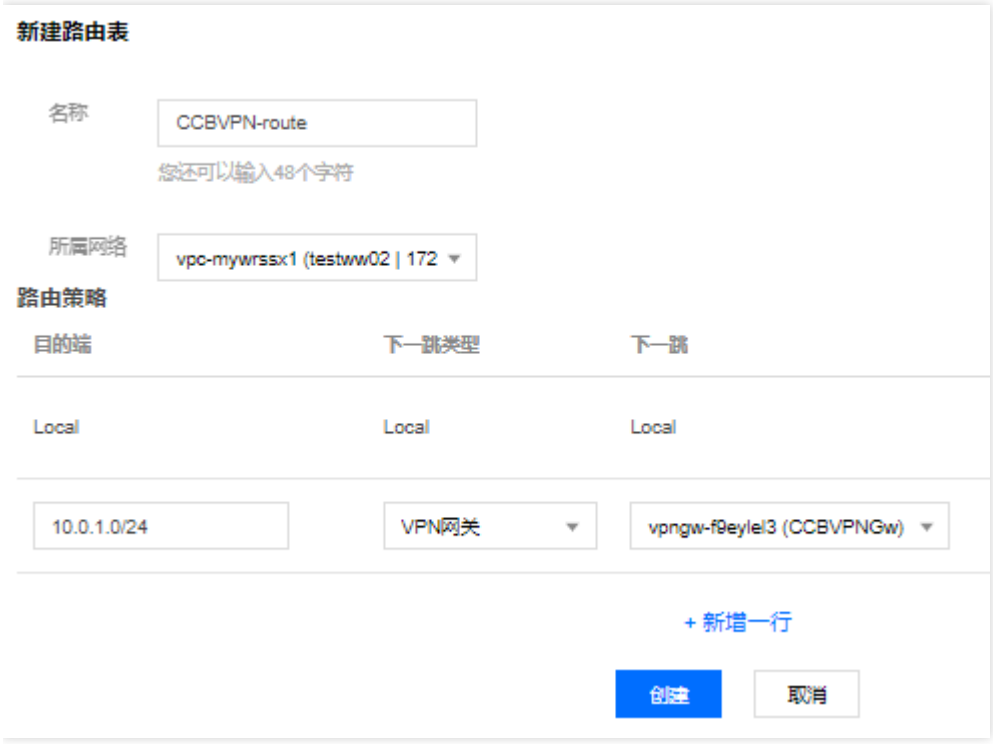
第五步:修改路由表

截止至第四步，我们已经将一条 VPN 通道配置成功，但是由于您还未将子网 A 中的流量路由指向 VPN 网关，子网 A 中的网段还不能与 IDC 中的网段通信。现在配置路由:

1) 登录云平台控制台点击导航条【私有网络】，进入私有网络控制台。

2) 点击左导航栏中【子网】，在列表的上端选择私有网络 CCBVPC 所在武汉和私有网络 CCBVPC，点击子网 A 所关联的路由表 ID 进入该路由表的详情页。

3) 点击【编辑按钮】，点击【新增一行】，输入目的端网段(10.0.1.0/24)，下一跳类型 选择【VPN 网关】，再选择刚刚创建的 VPN 网关 CCBVPNGw。



4) 点击【保存】，即完成需要通信的子网的出包路由设定。

第六步:VPN 通道激活

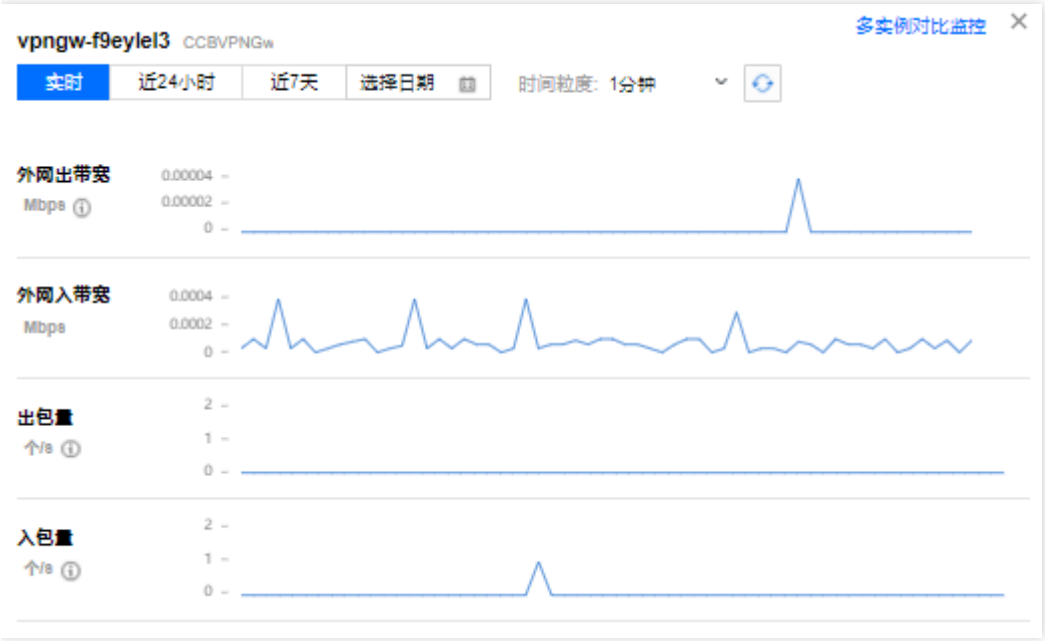
用 VPC 内的云服务器 ping 对端网段中的 IP 以激活 VPN 通道。如:CCBVPC内的子网 A 中的云服务器ping 10.0.1.17

操作指南
查看监控数据

最近更新时间: 2023-03-20 15:18:11

VPN 通道和 VPN 网关提供监控数据查看功能。

1) 登录云平台控制台，点击导航条【私有网络】，进入私有网络控制台；
2) 点击左导航栏中【VPN 连接】-【VPN 网关】或者【VPN 通道】选项卡；
3) 点击列表页中监控一列的图标查看监控数据。



设置告警

最近更新时间: 2023-03-20 15:18:06

VPN 通道提供告警功能:

1) 登录云平台控制台，点击顶部导航条【云产品】-【管理与审计】-【云监控】，选择左导航栏内的【告警配置】-【告警策略】，点击【新增】。
2) 填写告警策略名称，在策略类型中选择【私有网络】-【VPN通道】/【VPN网关】，添加告警触发条件，可设置指标告警或事件告警。
3) 关联告警对象：选择告警接收组，保存后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，您将接受到短信/邮件等通知，同时可以在左导航【告警历史】中查看。有关告警的更多信息，请参考创建告警。

查看 /修改VPN 网关详细信息

最近更新时间: 2023-03-20 15:18:06

1) 登录云平台控制台，点击导航条【私有网络】，进入私有网络控制台；
2) 点击左导航栏中【VPN 连接】-【VPN 网关】选项卡；
3) 点击 VPN 网关 ID 即可进入 VPN 网关详情页查看 VPN 网关信息，并做修改；

修改 VPN 通道配置

最近更新时间: 2023-03-20 15:18:06

1) 登录云平台控制台，点击导航条【私有网络】，进入私有网络控制台；
2) 点击左导航栏中【VPN 连接】-【VPN 通道】选项卡；
3) 点击 VPN 网关 ID 即可进入 VPN 网关详情页查看 VPN 网关信息；
4) 您可以在基本信息页中修改基本信息和 SPD 策略，或者您可以在高级配置修改 IKE 和 IPsec 配置。

常见问题

VPN 网关是如何实现的，可用性如何?

最近更新时间: 2023-03-20 15:18:11

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，建议使用专线接入产品。

可否同时使用专线和IPsec VPN连接到同一私有网络?

最近更新时间: 2023-03-20 15:18:11

可以。网络流量具体根据私有网络子网路由表设计流动。

使用VPN产品时，数据传输量是否有限制?

最近更新时间: 2023-03-20 15:18:11

没有限制，您可以传输任意数量的数据，最大速度为您选择的带宽上限。

VPN网关长期处于“发货中”状态或创建失败，是什么原因?

最近更新时间: 2023-03-20 15:18:11

新建VPN网关时所需时间较长，若5分钟内处于“发货中”状态时，请耐心等待；若长期处于“发货中”，最终VPN网关创建失败时，请确认账户下是否存在弹性公网IP，并反馈联系平台产品团队人员。

通道状态显示“未联通”，是什么原因?

最近更新时间: 2023-03-20 15:18:11

在您配置通道的过程中通道状态显示“未联通”，先检查路由表中的下一跳是否指向 VPN 网关，再用 VPC 内的云服务器 ping 对端网段中的 IP 以激活 VPN 通道。如在VPN产品使用过程中，通道状态显示“未联通”，请确认本端及对端通道是否有对配置进行修改，并及时联系云计算运营处工作人员。

当填写SPD策略时提示“SPD策略冲突”时该怎么办?

最近更新时间: 2023-03-20 15:18:11

填写【本端网段、对端网段】提示“用户SPD策略冲突”的原因是您的本端网段与对端网段重叠、或者每个本端网段对应的多个对端网段重叠，请调整您的对端网段来满足要求，详情请见上文SPD策略。