专线接入

产品简介

产品文档

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2024-01-13 16:02:36

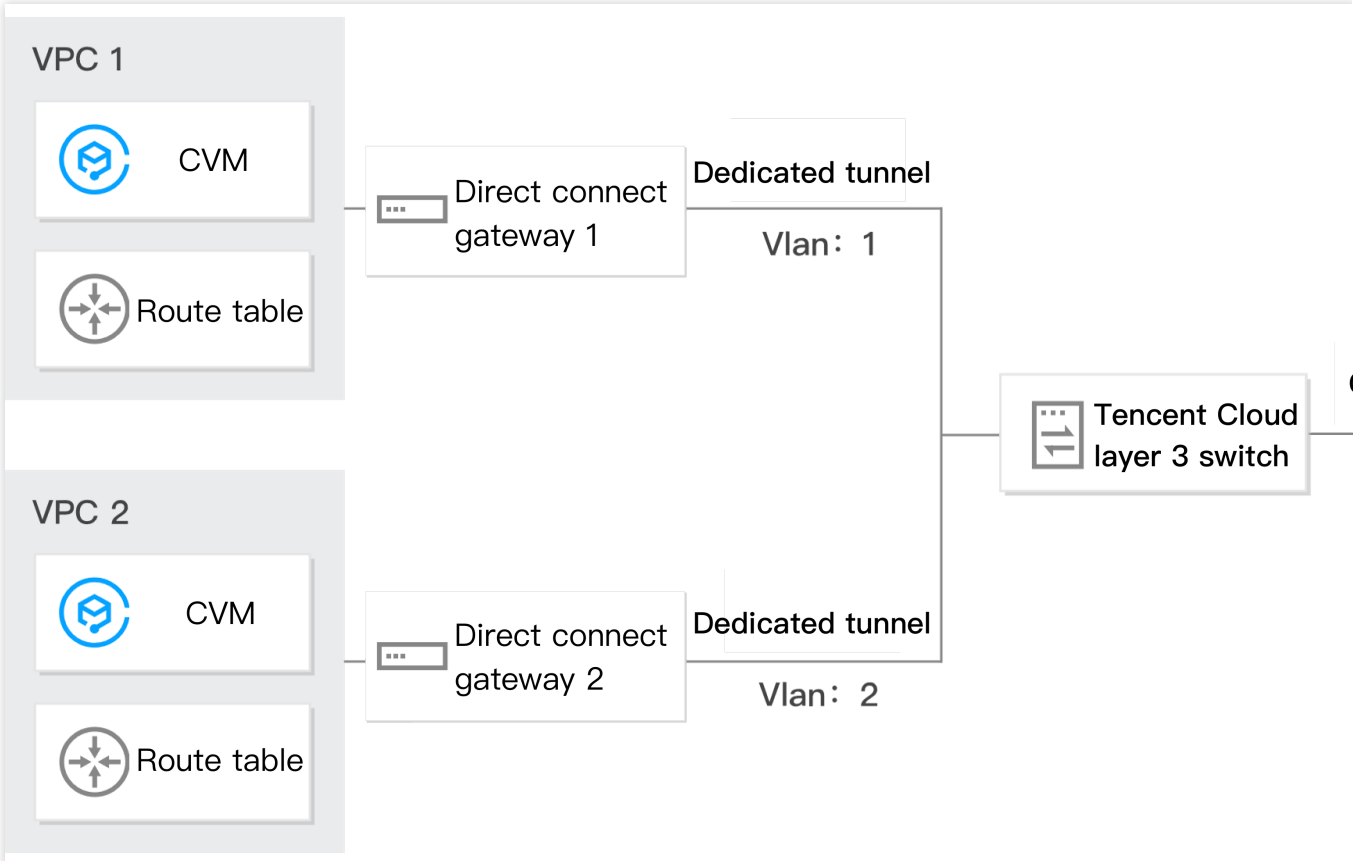
什么是专线接入

专线接入提供了一种快速安全连接腾讯云与本地数据中心的方法。用户可以通过一条物理专线，一次性打通位于多地域的腾讯云计算资源，实现灵活可靠的混合云部署。

专线部署混合云（一）

使用传统的专用通道打通用户 IDC 与云上 VPC。

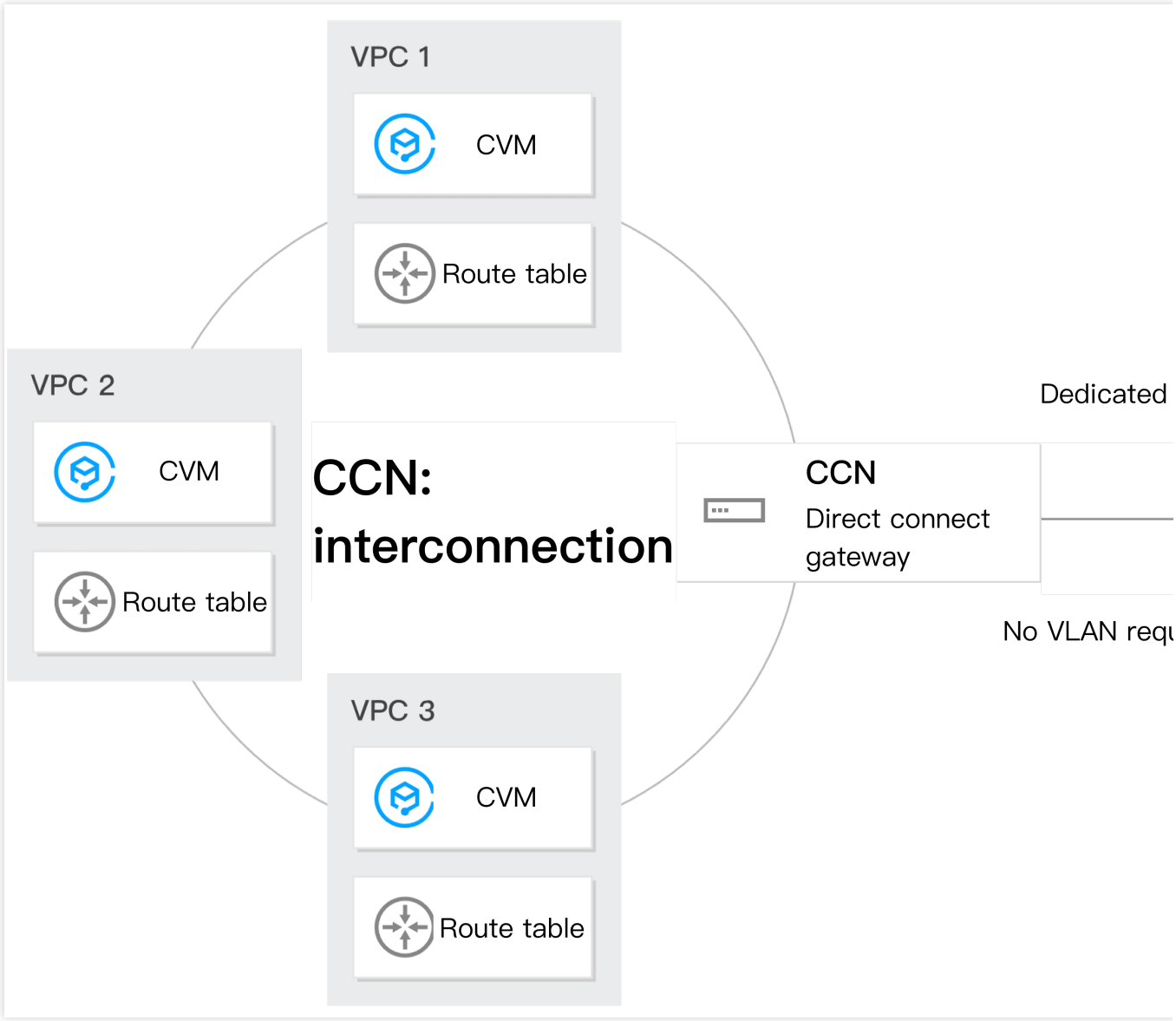
如果一根物理专线需要打通多个 VPC，您需要通过不同的 VLAN ID 分别创建专用通道来连接多 个VPC。



专线部署混合云（二）

使用云联网产品实现互通。

优势：您只需要创建一个通道连接云联网专线网关，然后把专线网关加载到云联网，即可实现云联网内的多个网络实例间全互通，操作简单。



组成部分

专线接入由物理专线、专用通道和专线网关组成。

物理专线

连接腾讯云与本地数据中心的物理线路连接。物理专线支持双线热备接入，双线接入点供电，网络管道完全隔离。

专用通道

专用通道是物理专线的网络链路划分。用户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

私有网络的专线流量出入口，可以通过接入多个专用通道与多个不同的 IDC 互联。专线网关通过集群方式实现，全路无单点故障风险，满足金融级网络互联要求。

专线网关是连接私有网络与物理专线的桥梁，您可以在物理专线内创建一条关联至某个专线网关的专用通道。

专线网关可以连接来自多个物理专线的专用通道，从而与您的多个本地数据中心互通。

用户可以在专线网关控制台为每个私有网络创建专线网关，每个私有网络最多支持创建2个专线网关（标准型和 NAT 型各1个），该专线网关可以连接来自不同物理专线的专用通道申请需求。

较 IPsec VPN 的优势与区别

优势	专线接入	IPsec VPN
稳定的网络延时	网络延时可靠有保证，接入网络基于专用线路，您可以通过固定的路由配置，免去拥堵或故障绕行带来的延时不稳定困扰。	接入网络连接基于 Internet，网络高峰链路阻塞时，可能会导致路由绕行，延时不稳定。
高可靠的容灾接入	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，满足您高于99.95%可用性的要求。	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	单线路最大支持100Gbps带宽连接，还可接入多条10Gbps链路做网络负载均衡，无理论上限。	单网关最大支持1Gbps带宽上限，私有网络支持多 VPN 网关配置，可通过多 VPN 网关配置，满足大于1Gbps的 VPN 接入。
安全性高	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。	网络传输基于 IKE 协议的预共享密钥加密，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	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，解决多方网络互联时的地址冲突难题。	暂不支持。

产品功能

最近更新时间：2024-01-13 16:02:36

物理专线

连接腾讯云与本地数据中心的物理线路连接，您可以通过第三方网络服务商，在您的数据中心和腾讯云专线网络接入点间建立网络连接。

专用通道

专用通道是物理专线的网络链路划分。
您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与物理专线建立专用通道的出入口，私有网络支持最多2个专线网关（标准型和 NAT 型各1个）。
专线网关可以和多个物理专线间建立专用通道，实现连接多地的混合云部署。

网络地址转换（NAT）

网络地址转换是混合云连接时，应对专线两端 IP 冲突问题的一种解决方案。您可以在专线网关上配置网络地址转换规则，网络地址转换（NAT）包含 IP 转换和 IP 端口转换两种。

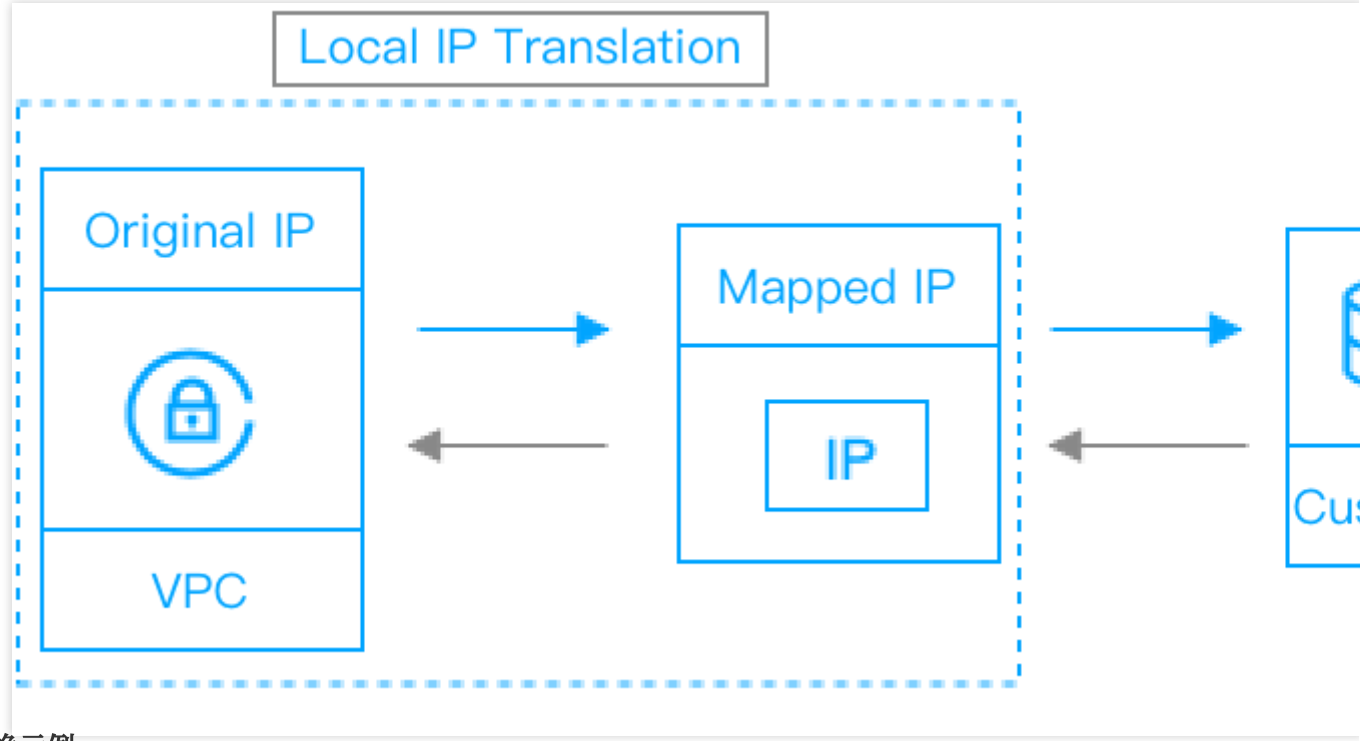
IP 转换

IP 转换指将源 IP 转换为新的 IP，实现网络互访，分为**本端 IP 转换**和**对端 IP 转换**。
IP 转换不区分源、目的方向，映射 IP 既可以主动访问对端，也可以被对端主动访问。

本端 IP 转换

1. 转换说明
本端 IP 转换指私有网络内源 IP 映射为新 IP，并以新 IP 身份与专线对端互访。
您可以配置多条本端 IP 转换规则，并为每条本端 IP 转换规则配置网络 ACL，网络 ACL 支持源端口、目的 IP、目的端口配置。
注意：

网络地址转换规则仅对符合 ACL 限制的网络请求生效。
本端 IP 转换不限制网络请求的方向，可以是私有网络主动访问专线对端，也可以是专线对端主动访问私有网络。



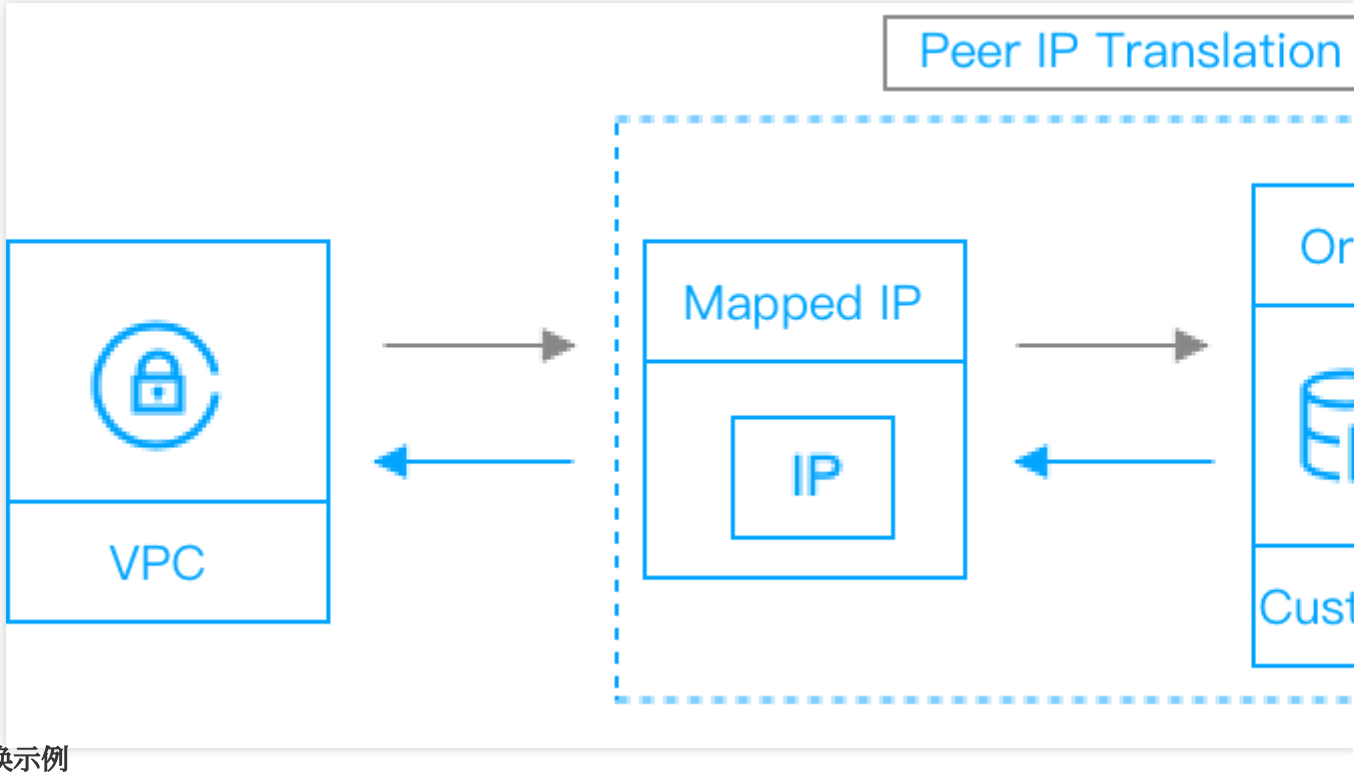
2. 转换示例

私有网络内 IP A `192.168.0.3` 映射为 IP B `10.100.0.3`，则 IP A 对专线对端的主动访问网络包源 IP 将自动修改为 `10.100.0.3`，所有专线对端访问的 `10.100.0.3` 的网络包将自动指向 IP A `192.168.0.3`。

对端 IP 转换

1. 转换说明

对端 IP 转换指用户 IDC 内源 IP 映射为新 IP，并以新 IP 身份与私有网络内 IP 互访。
和本端 IP 转换不同，对端 IP 转换不支持网络 ACL 限制，因此，一旦配置了对端 IP 转换规则，将对所有专用通道对端生效。
对端 IP 转换不限制网络请求的方向，可以是私有网络主动访问专线对端，也支持专线对端主动访问私有网络。



2. 转换示例

专线对端 IP D `10.0.0.3` 映射为 IP C `172.16.0.3`，则 IP D `10.0.0.3` 主动访问私有网络的网络包源 IP，将自动修改为 IP C `172.16.0.3`，所有私有网络访问 IP C `172.16.0.3` 的网络包，将自动指向专线对端 IP D `10.0.0.3`。

注意：

配置本端、对端 IP 转换后，专线网关仅会将转换后的 IP 路由下发至专线对端，因此，未配置本端、对端 IP 转换的源 IP，将无法 ping 通专线对端。但专线网关无法代替专业的网络防火墙，如果您需要高级的网络防护，请在私有网络内配置安全组和网络 ACL 策略，同时在您的 IDC 机房部署专业的物理网络防火墙设备。

当专线网关同时配置对端 IP 转换时，本端源 IP 端口转换 ACL 规则的 **目的 IP** 需要写 **对端 IP 转换的映射 IP**，而不是源 IP。

IP 端口转换

IP 端口转换指将源 IP 端口映射为新 IP 端口，并以新 IP 端口实现网络互访，包含**本端源 IP 端口转换**、**本端目的 IP 端口转换**。

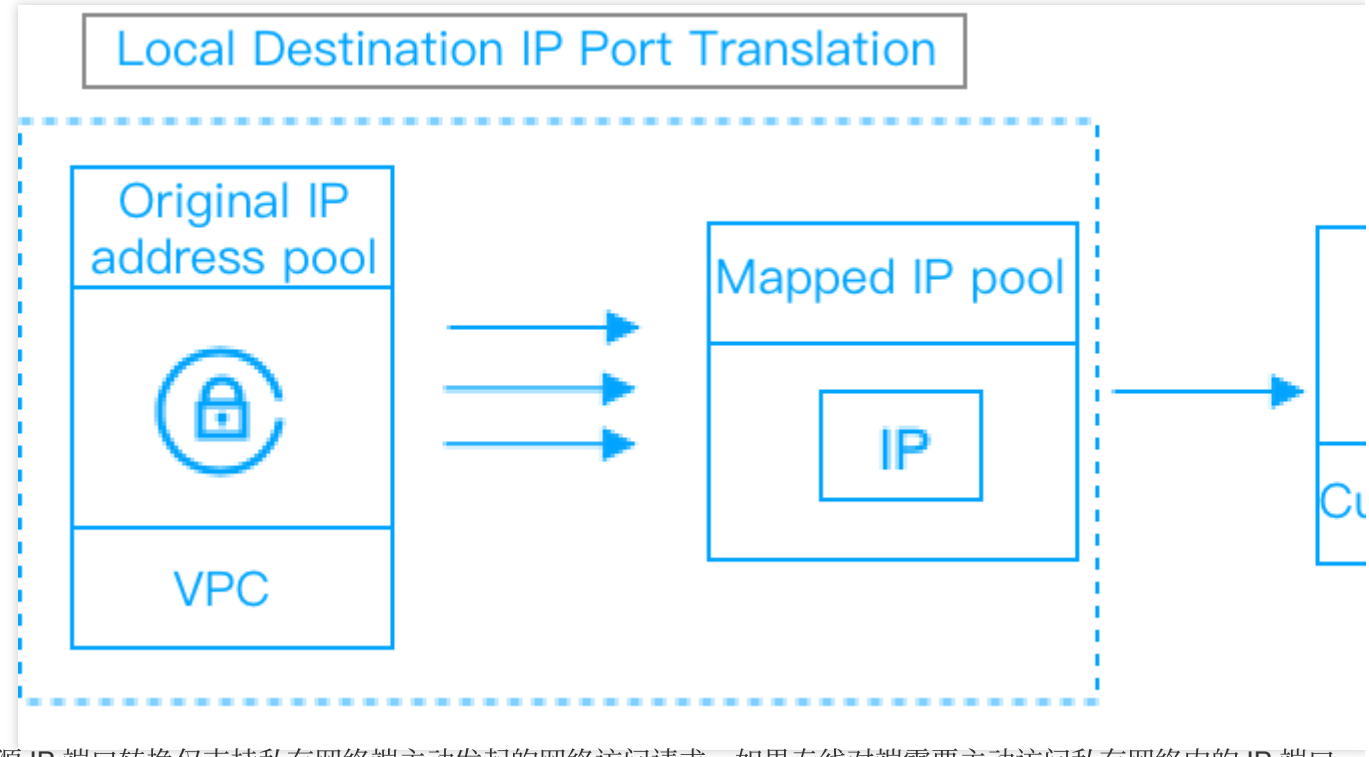
IP 端口转换强调方向性，源 IP 端口转换指主动外访，目的 IP 端口转换指被对端主动访问。

本端源 IP 端口转换

1. 转换说明

本端源 IP 端口转换指私有网络内 IP 通过专线网关主动外访时，以指定 IP 池内随机 IP 的随机端口访问专线对端的用户 IDC。

本端源 IP 端口转换支持配置 ACL 规则，只有符合 ACL 规则的网络访问才会匹配地址池转发规则。通过为地址池配置不同的 ACL 规则，您可以灵活配置多个第三方接入时的网络地址转换规则。



本端源 IP 端口转换仅支持私有网络端主动发起的网络访问请求，如果专线对端需要主动访问私有网络内的 IP 端口，需要额外进行本端目的 IP 端口转换配置。本端源 IP 端口转换私有网络主动发起的网络请求为有状态连接，不用考虑网络回包问题。

2. 示例：

私有网络 C 网段为 `172.16.0.0/16`，通过专线连接第三方银行 A 和 B，其中银行 A 对端网段为 `10.0.0.0/28`，要求对接网段为 `192.168.0.0/28`；银行 B 对端网段为 `10.1.0.0/28`，要求对接网段为 `192.168.1.0/28`。则可以按照下面配置两条本端源 IP 端口转换：

地址池 A `192.168.0.1 - 192.168.0.15`；ACL 规则 A：源 IP `172.16.0.0/16`，目的 IP `10.0.0.0/28`，目的端口 ALL。

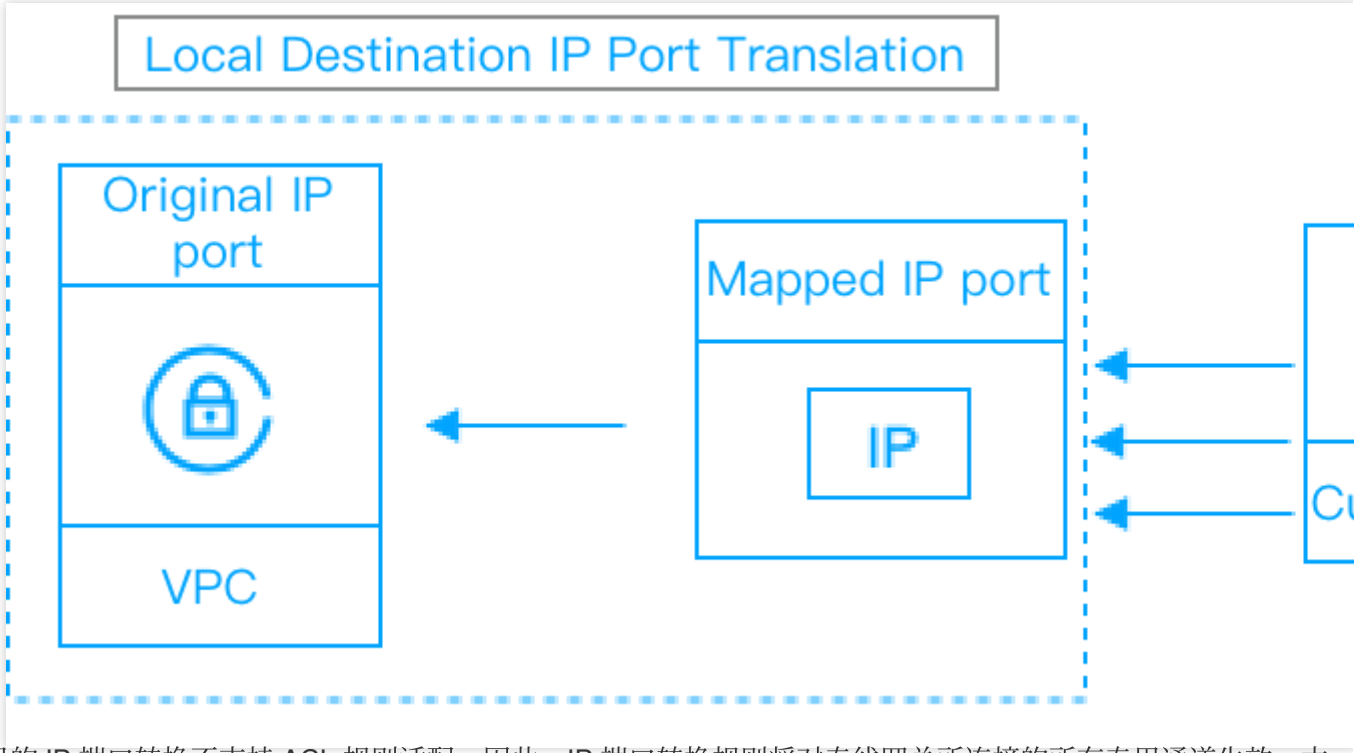
地址池 B `192.168.1.1 - 192.168.1.15`；ACL 规则 B：源 IP `172.16.0.0/16`，目的 IP `10.1.0.0/28`，目的端口 ALL。

则私有网络内主动访问 A、B 的网络请求，会根据 ACL 规则 A、B 分别转换为对应地址池的随机端口，访问对应的专用通道。

本端目的 IP 端口转换

1. 转换说明

本端目的 IP 端口转换是专线对端主动访问私有网络的一种方法，将私有网络内指定 IP 的指定端口映射为新的 IP 和端口，专线对端则只可以通过访问映射后 IP 端口来与私有网络内指定 IP 端口通信，其他 IP 端口则不对专线对端暴露。



本端目的 IP 端口转换不支持 ACL 规则适配，因此，IP 端口转换规则将对专线网关所连接的所有专用通道生效。本端目的 IP 端口转换仅对专用通道对端主动访问私有网络生效，如果私有网络需要主动访问专线对端，可以配置本端源 IP 端口转换。本端目的 IP 端口转换的网络请求为有状态连接，无需考虑网络回包的问题。

2. 转换示例

私有网络 C 的网段为 `172.16.0.0/16`，只希望开放若干端口给专线对端主动访问，则可以按照下面方案进行配置：

映射 A 源 IP 端口 `172.16.0.1:80` ；映射 IP 端口 `10.0.0.1:80` 。

映射 B 源 IP 端口 `172.16.0.0:8080` ；映射 IP 端口 `10.0.0.1:8080` 。

则专线对端可以主动访问 `10.0.0.1:80` 、 `10.0.0.1:8080` 端口，实现对私有网络内 `172.16.0.1:80` 、 `172.16.0.0:8080` 两个端口的主动访问。

注意：

配置本端源、目的 IP 端口转换后，专线网关仅会将转换后 IP 端口路由下发至专线对端，因此，未配置的本端 IP 端口，将无法主动发起请求或被动接受请求。但专线网关无法代替专业的网络防火墙，如果您需要高级的网络防护，请在私有网络内配置安全组和网络 ACL 策略，同时在您的 IDC 机房部署专业的物理网络防火墙设备。

当同时配置 IP 转换和 IP 端口转换时，优先匹配 IP 转换，IP 转换无匹配选项时，才会继续匹配 IP 端口转换。

当专线网关同时配置对端 IP 转换时，本端源 IP 端口转换 ACL 规则的**目的 IP** 需要写**对端 IP 转换的映射 IP**，而不是源 IP。

应用场景
容灾部署

最近更新时间：2024-01-13 16:02:36

应用场景

用户已经具有大规模应用，其核心问题不再是基础设施部署速度无法满足业务增长，更多的是从稳定性、可靠性等方面，寻求从单中心向多中心化发展，通过消灭单点，解决单数据中心故障带来的业务风险。

用户核心需求：

多地容灾，提高基础设施可靠性。

快速部署，减少基础设施建设周期。

存量数据中心利旧，降低运行成本（已有服务器可继续使用）。

解决方案

混合云容灾部署

异地部署数据中心

本地数据中心和公有云数据中心构建主备集群。

数据同步

通过专线或 VPN 同步数据，避免单中心失效。

流量切换

通过 DNS 将流量切换至有效中心，提供有损但不中断的基础业务服务。

云上两地三中心容灾部署

跨可用区部署

您可以在同一个私有网络内的不同可用区创建子网、部署服务。不同可用区的子网之间可以同步数据（使用不同可用区的目标是保证故障相互隔离）。

跨地域部署

为了实现多地容灾，避免单地域故障扩散，高容灾保障，您可以在另一地域的私有网络内部署同样的服务。

跨地域高速互联

两个地域的私有网络之间通过跨地域对等连接实现跨地域互通。

操作步骤

混合云容灾部署

1. 在腾讯云上创建私有网络，部署数据中心，详情请参见 私有网络操作指南。
2. 通过专线同步企业本地数据中心和云上私有网络数据中心，详情请参见 专线接入操作指南。
3. 故障发生时，通过 DNS 将流量切换有效的数据中心。

云上两地三中心容灾部署

1. 跨可用区部署。

您可以在同一个私有网络内的不同可用区创建子网，部署主备同步的服务。不同可用区的子网之间可以同步数据，使用不同可用区的目标是保证故障相互隔离。详情请参见 子网操作指南。

2. 跨地域部署。

为了实现多地容灾，避免单地域故障扩散，您可以在另外一个地域的私有网络内部署同样的服务。详情请参见 私有网络操作指南。

3. 跨地域高速互联。

创建跨地域对等连接，实现两个私有网络高速同步数据，详情请参见 对等连接操作指南。

混合云部署

最近更新时间：2024-01-13 16:02:36

根据连接企业数据中心和私有网络的不同连接需求，腾讯云提供 VPN 连接和专线接入服务，主要区别如下：

VPN 连接

利用公网和 IPsec 协议，在您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、阻塞等公网质量问题而中断，当用户业务对网络连接质量要求不高时，VPN 连接是一种快速部署的高性价比选择。

专线接入

为您提供一个专用的专线网络连接方案，施工时间较长，但可以提供高质量、高可靠的网络连接服务。当您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。

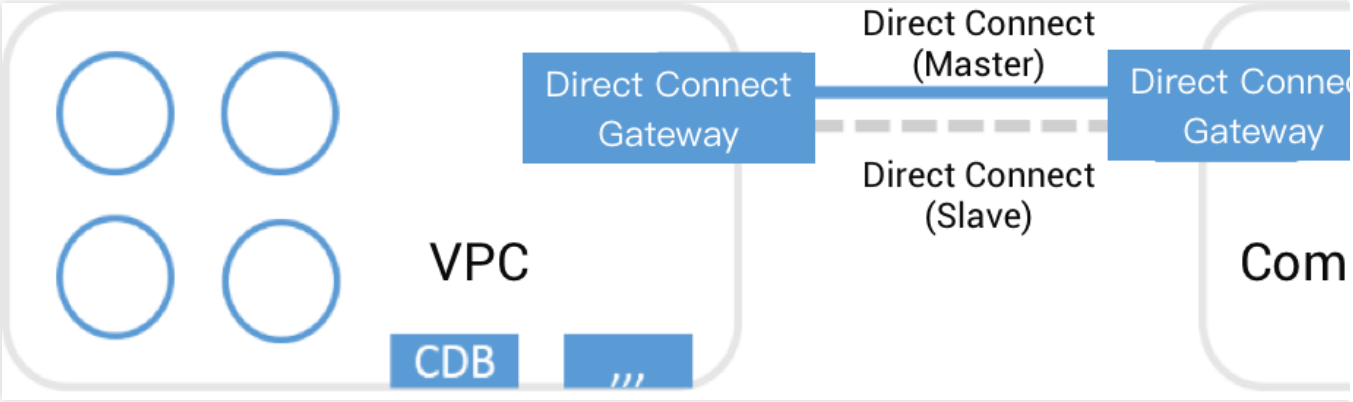
下面将为您详细介绍专线接入部署混合云。

应用场景

专线接入提供了一种快速安全连接腾讯云与本地数据中心的方法，用户可以通过一条物理专线一次性打通位于多地域的腾讯云计算资源，实现灵活可靠的混合云部署。

如果您需要为专线设置备份，有两种方式：

双专线接入备份，腾讯云支持主备故障切换（主备）配置。



VPN连接作为专线链路备份（主备）。

注意：

私有网络和数据中心的 **网段重叠不影响** 双方通信，因为腾讯云专线网关支持 NAT 功能，详情请参见 产品功能。

解决方案

云上数据中心

在腾讯云创建的某个私有网络，使用云服务器和云数据部署云上数据中心。

连接方式

通过物理专线接入实现私有网络中的数据中心与您自有 IDC 的内网融合。

连接备份方式

双专线备份 / VPN 连接备份。

操作步骤

如果您选择使用专线接入打通您的数据中心和在腾讯云上 VPC 中数据中心，那么您需要完成以下步骤：

1. 创建物理专线。
2. 创建专用通道。
3. 创建专线网关接入专用通道，从而打通数据中心和您的 VPC。
4. 配置专线 NAT（可选）。
5. 配置需要通信的子网所关联的路由表。
6. 您可以选择创建多条物理专线或者 VPN 连接，实现单条的专线备份。

详情请参见 快速入门。

使用限制

最近更新时间：2024-01-13 16:02:36

资源限制

资源	限制	可申请高配额	说明
物理专线 / 用户	10个	是	每个用户可接入的物理专线数不超过10个
专用通道 / 物理专线	5个	是	每个物理专线中创建专用通道数不超过5个
专线网关 / 私有网络	2个（标准型和 NAT 型各1个）	否	每个私有网络中配置的专线网关数不超过2个。
本端 IP 转换 / 专线网关	100条	是	每个专线网关配置的本端 IP 转换数不超过100条。
对端 IP 转换 / 专线网关	100条	是	每个专线网关配置的对端 IP 转换数不超过100条。
本端源 IP 端口转换 IP 数 / 专线网关	20个	是	每个专线网关配置的本端源 IP 端口转换数不超过20个。
本端目的 IP 端口转换 / 专线网关	100条	是	每个专线网关配置的本端目的 IP 端口转换数不超过100条。
专用通道静态路由条目数	专用通道1.0 ：20条	否	专用通道静态路由条目数不超20条。
	专用通道2.0 ：50条	是	专用通道静态路由条目数不超50条，如需调整额度请提 工单申请。
专用通道 BGP 路由条目数	专用通道1.0 ：100条	否	专用通道 BGP 路由条目数不超100条。
	专用通道2.0 ：100条	是	专用通道 BGP 路由条目数不超100条，如需调整额度请提 工单申请。

接入限制

专线接入

新建专线网关时，IP 转换和 IP 端口转换内容默认为空，此时 IP 转换与 IP 端口转换均不生效。

专用通道支持 BGP 路由和静态路由两种路由方式。

发布路由时请注意如下限制：

为了提高您网络的精细化调度能力，请勿发布以下路由：

专线

1.0 `9.0.0.0/8`，`10.0.0.0/8`，`11.0.0.0/8`，`30.0.0.0/8`，`100.64.0.0/10`，`131.87.0.0/16`，`172.16.0.0/12`，`192.168.0.0/16`。

注意：

若发布大网段路由，专线网关将直接拒收。

您可以将以上大段路由拆分为如下发布：

`9.0.0.0/8`

拆分为：`9.0.0.0/9` + `9.128.0.0/9`。

`10.0.0.0/8`

拆分为：`10.0.0.0/9` + `10.128.0.0/9`。

`11.0.0.0/8`

拆分为：`11.0.0.0/9` + `11.128.0.0/9`。

`30.0.0.0/8`

拆分为：`30.0.0.0/9` + `30.128.0.0/9`。

`100.64.0.0/10`

拆分为：`100.64.0.0/11` + `100.96.0.0/11`。

`131.87.0.0/16`

拆分为：`131.87.0.0/17` + `131.87.128.0/17`。

`172.16.0.0/12`

拆分为：`172.16.0.0/13` + `172.24.0.0/13`。

`192.168.0.0/16`

拆分为：`192.168.0.0/17` + `192.168.128.0/17`。

专线2.0

`127.0.0.0/8`、`224.0.0.0/4`、`240.0.0.0/4`、`255.255.255.255`、`169.254.0.0/16`（`169.254.64.0/23`除外）。

边界 IP 所在网段的子网和网段内的 IP。如有互访需要，请 提交工单开启“互联 IP 重分布”。

IP 转换

IP 地址池不可以在专线网关所在私有网络的 CIDR 范围内。

多个 IP 地址池的 ACL 规则不可以重叠，否则会导致网络地址转换冲突。

多个 IP 地址池之间 IP 不可以重叠。

IP 地址池仅支持单 IP 或连续 IP，且连续 IP 的 `/24` 网段需保持一致，即支持 `192.168.0.1 - 192.168.0.6`，不支持 `192.168.0.1 - 192.168.1.2`。
地址池不支持广播地址（`255.255.255.255`）、D 类地址 `224.0.0.0 - 239.255.255.255`、E 类地址 `240.0.0.0 - 255.255.255.254`。
本端源 IP 端口转换最大支持100个 IP 地址池，每个地址池支持最大20条 ACL 规则（如有需求，可以 提交工单 申请提高配额）。
当您需要从 IP 转换切换为 IP 端口转换时，请清空源 IP 转换规则，刷新页面后，即可编辑 IP 端口转换规则。

IP 端口转换

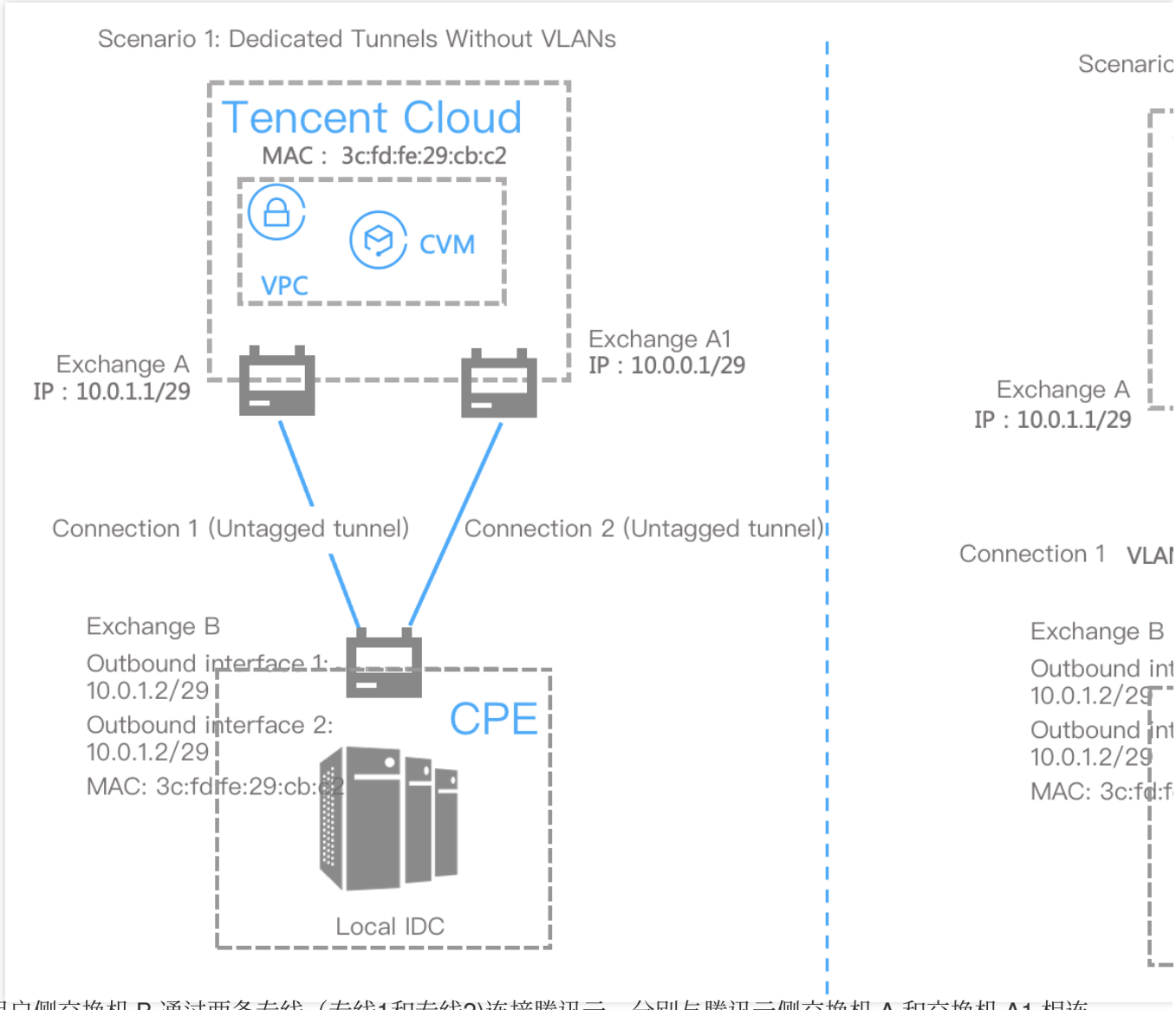
源 IP 必须在专线网关所在私有网络 CIDR 范围之内。
源 IP 端口唯一，即私有网络内同一 IP 端口只能唯一映射为一个 IP 端口。
映射 IP 端口不可以在私有网络 CIDR 范围之内。
映射 IP 端口不可以重复，即不存在一个 IP 端口映射多个私有网络 IP 端口。
源 IP 和映射 IP 不支持广播地址 `255.255.255.255`、D 类地址 `224.0.0.0 - 239.255.255.255`、E 类地址 `240.0.0.0 - 255.255.255.254`。
本端目的 IP 端口转换最大支持100个 IP 端口映射（如有需求，可以 提交工单 申请提高配额）。
同时配置 IP 转换和 IP 端口转换时，如果同时命中，优先匹配 IP 转换。

网络约束

在使用物理专线连接用户 IDC 和腾讯云时，对两端的 MAC 地址有一定要求，为了确保网络正常通行，请悉知如下约束。

MAC

腾讯云侧接入交换机固定MAC地址为3c:fd:fe:29:cb:c2，用户IDC侧接入设备的 MAC 地址请勿使用该 MAC 地址，以防因 MAC 地址冲突而出现 MAC 地址漂移（交换跳变）问题，致使网络不可达、响应慢、无响应等网络现象。
说明：
MAC 地址漂移（交换跳变）是指设备上同一 VLAN 内2个出接口学习到了同一个 MAC 地址，后学到的 MAC 地址覆盖先学到的 MAC 地址现象，致使 MAC 地址不稳定。
如下是产生 MAC 地址漂移的场景：



图中用户侧交换机 B 通过两条专线（专线1和专线2)连接腾讯云，分别与腾讯云侧交换机 A 和交换机 A1 相连。腾讯云返回给用户 IDC 的报文在交换机 B 处发生 MAC 地址漂移。

接入约束

为了防止因网络环路产生网络拥塞问题，建议您使用3层网络子接口对接腾讯云专线设备。

相关产品

最近更新时间：2024-01-13 16:02:36

相关产品信息，请参见下表：

产品名称	与专线接入的关系
私有网络	可物理专线接入，实现私有网络中数据中心与您自有的 IDC 的内网融合
云联网	云联网产品支持单专用通道打通云上多个 VPC
网络 ACL	可配置多条本端 IP 转换规则，并为每条本端 IP 转换规则配置网络 ACL
路由表	混合云部署需要配置子网所关联的路由表

网络规划

最近更新时间：2024-01-13 16:09:21

搭建专线网络架构前，请先阅读本文了解物理线路规划信息。

背景信息

合理规划物理线路可以提升专线网络架构的稳定性和高可用性，例如在网络设备故障、端口异常/光模块故障、物理专线故障和接入点机房故障等场景下，把故障对业务的影响降到最低。常见故障的说明和造成原因如下：

故障类型	描述	造成原因
物理专线故障	物理专线不可通信或通信丢包严重。	物理专线损坏，例如因施工导致的线缆被误挖断。
端口异常/光模块故障	端口/光模块信息读取失败、硬件故障、软件故障导致的传输异常。	硬件故障：型号不匹配、接口受到污染或损伤。 软件故障：端口状态不为 UP、端口状态为 UP 但不接收或发送报文、端口频繁启停以及 循环冗余校验（CRC）错误。
网络设备故障	IDC 侧交换机或路由器不可用。	硬件故障：电源、端口、模块或线缆等故障。 软件故障：交换机/路由器系统错误、配置不当。
接入点机房故障	机房网络不通，接入点不可用。	地震、火灾等因素导致的机房无法正常工作。

规划思路

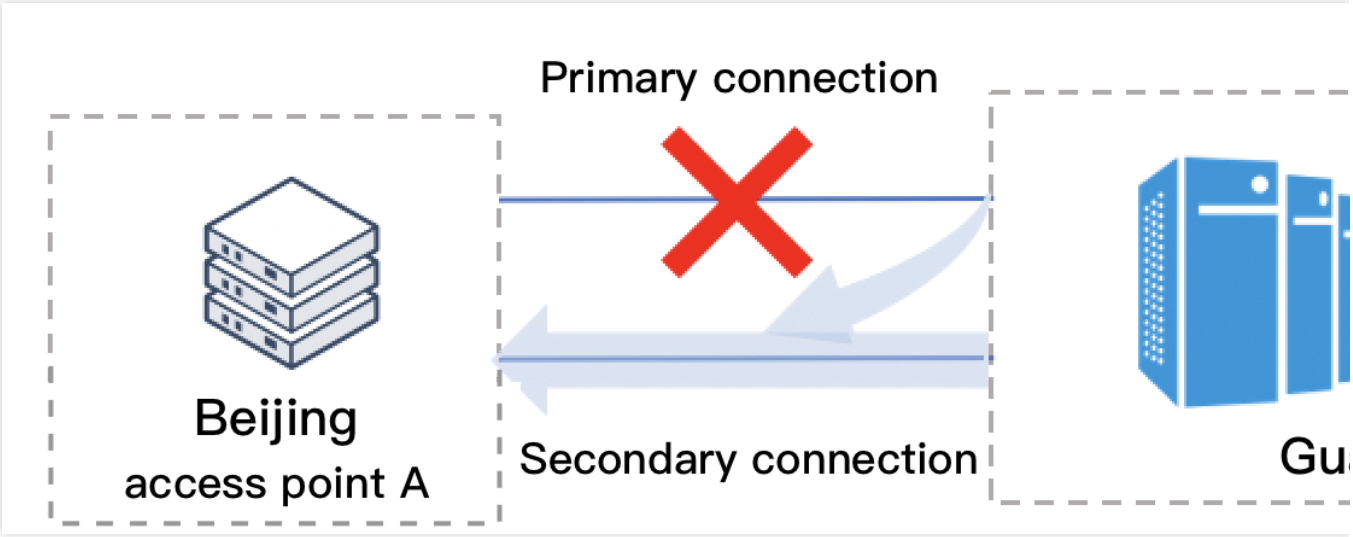
容量规划

容量规划的目标是以合理的成本满足业务带宽需求，保证在物理专线故障情况下，业务可以正常运行。容量规划建议如下：

申请物理专线数量是您实际需求的两倍。

每条物理专线使用率（当前峰值带宽值/物理专线带宽值*100%）不超过 50%。

例如某用户的业务带宽为3Mbps，则该用户可以针对每个腾讯云接入点申请两条带宽5Mbps的物理专线，每条物理专线使用率约为30%。当其中一条物理专线故障时，业务流量可以快速切换至备用专线，保证业务连续性。切换后备用专线使用率约为60%，仅线路负载临时性升高，业务数据无损。

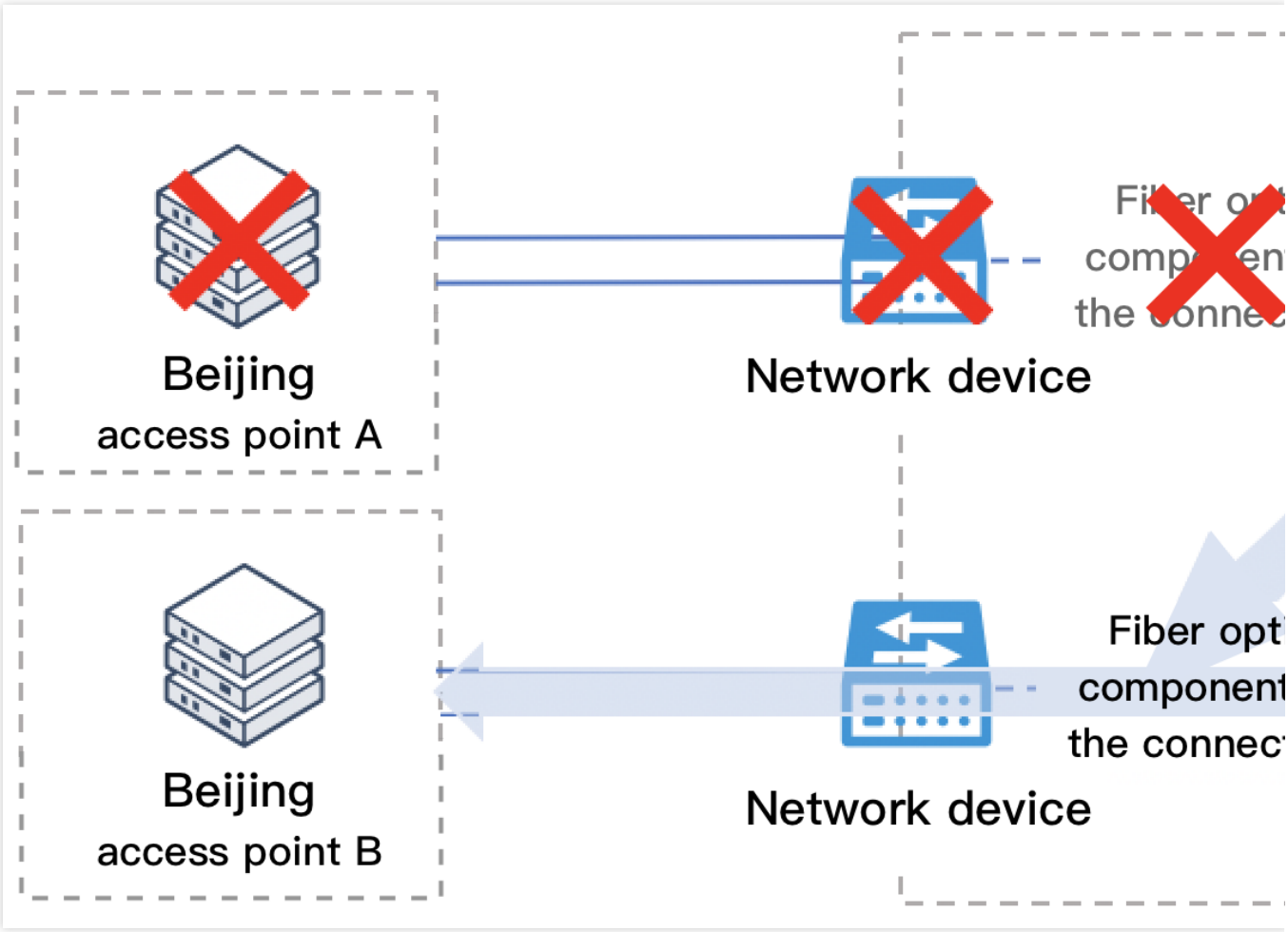


扩容规划

扩容规划的目标是以合理的成本满足业务流量增长的需求，根据扩容周期不同，扩容规划建议如下：
若需在短时间内完成扩容，创建物理专线时，可根据预估的业务带宽申请大规格的物理专线，以确保在业务流量骤增时，可以通过调整限速带宽来快速满足增长业务带宽需求，确保线上业务不受影响。
若无需在短时间内完成扩容，则可根据实际扩容需求新申请专线，扩容周期约2~3个月。
说明：
单次扩容超过100G的带宽需求需要更长的扩容时间，针对大带宽业务需要提前做好业务扩容计划。

容灾规划

容灾规划的目标是提高专线网络架构的高可用性，确保在各种故障场景下（如：端口异常/光模块故障、网络设备故障、接入点机房故障等），最大程度的降低对线上业务的影响。
为了避免单点故障，腾讯云建议您从接入点，物理线路、硬件设备等方面准备容灾规划：
接入点：本地 IDC 通过不同线路的物理专线与同地域两个腾讯云接入点连接。
物理线路：通过不同运营商的不同物理路径接入腾讯云接入点。
硬件设备：网络设备、光模块等组件均有冗余备份。
例如某用户按照 容量规划 要求，将本地 IDC 与同地域的两个腾讯云接入点进行连接，如下图所示。当接入点 A 的物理线路遇到端口异常/光模块故障、网络设备故障或接入点机房故障导致网络不通时，业务流量将快速切换至接入点 B 的物理线路，且业务数据不丢失，业务不中断。



模式举例

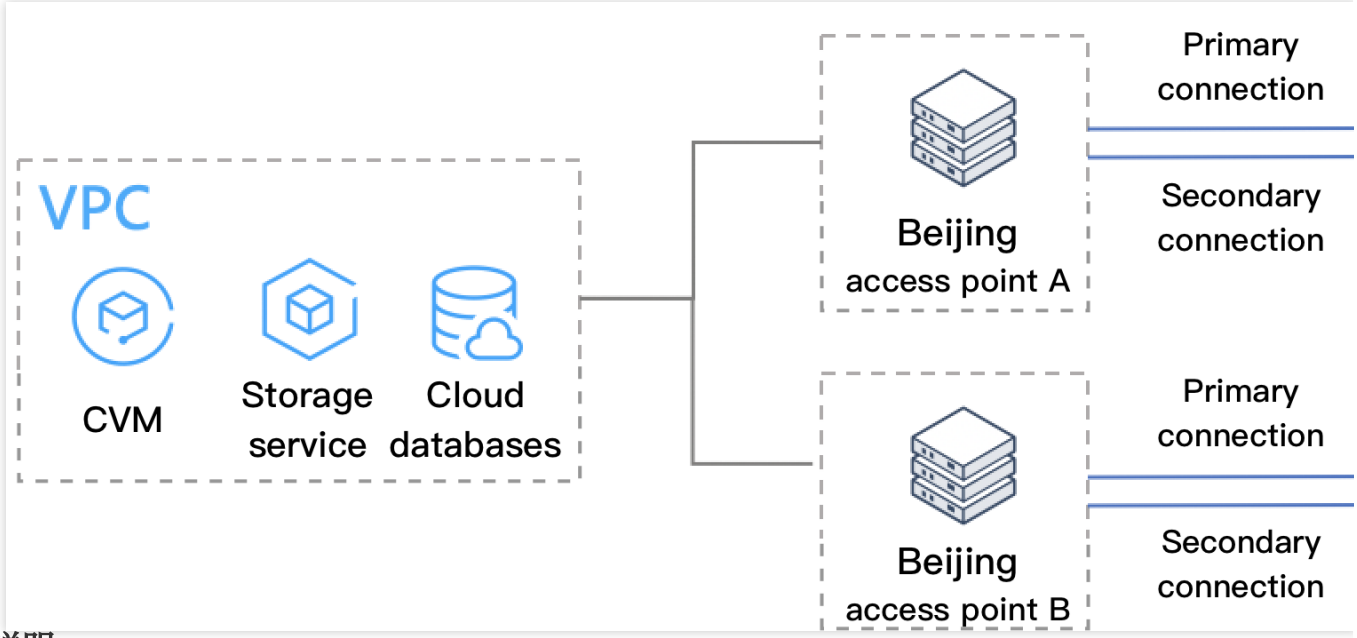
腾讯云总结了以下4种常用专线网络架构模式，帮助您进行网络规划。

模式	使用场景	业务弹性	可用性	成本
四线双接入点模式-推荐	适用于关键生产、实时数据交易等对业务可用性、弹性要求极高的场景。	高	高	高
双线双接入点模式-推荐	适用于对关键业务可用性和弹性较高的场景。	中	较高	中
双线单接入点模式	适用于非关键业务场景，例如云上开发和测试环境。	中	中	中
单线单接入点模式	适用于不需要高弹性和高可用性的非关键业务场景。	低	低	低

四线双接入点模式（推荐）

模式介绍

描述：四线双接入点模式中，用户 IDC 与同地域的两个腾讯云接入点连接，且与每个接入点连接均使用主备两条物理专线构建物理连接，再连接至腾讯云 VPC。
使用场景：适用于关键生产、实时数据交易等对业务可用性、弹性要求极高的场景。
成本：高。



容灾说明

在满足 规划思路 要求的情况下，四线双接入点模式的专线网络架构在各类故障场景下对业务的影响如下。

故障类型	业务影响
物理专线故障	物理专线负载率升高，业务不会中断。
端口异常/光模块故障	物理专线负载率升高，业务不会中断。
网络设备故障	物理专线负载率升高，业务不会中断。
接入点机房故障	物理专线负载率升高，业务不会中断。

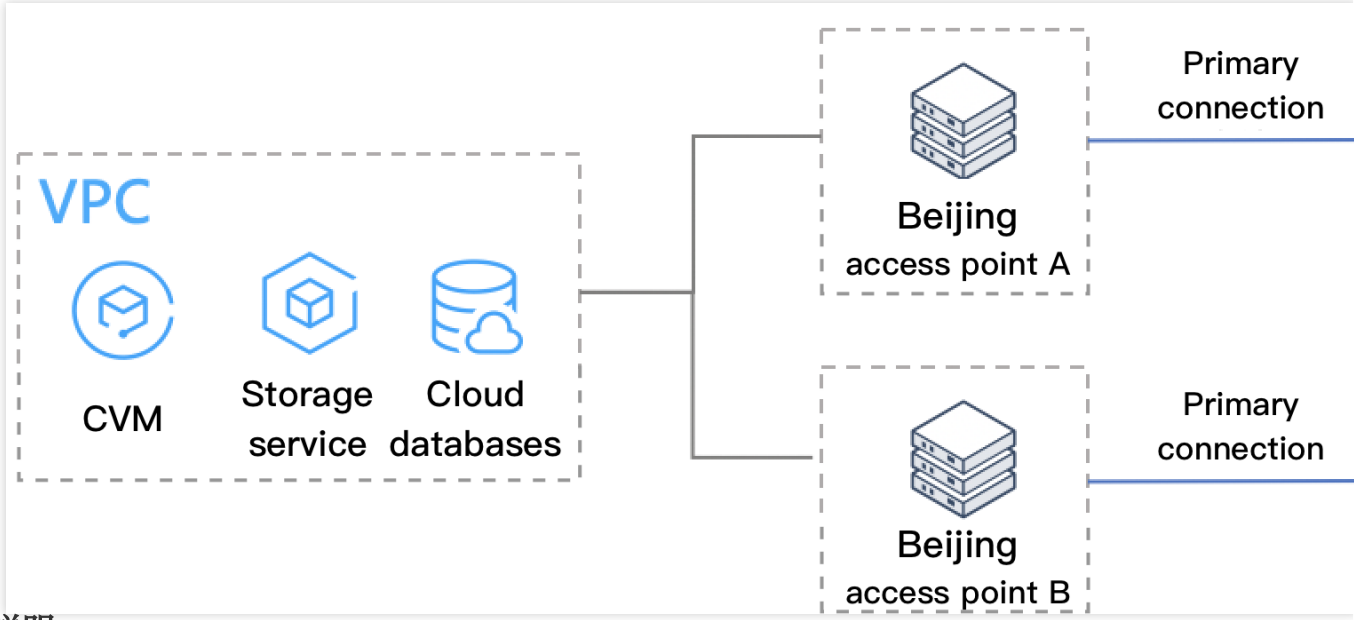
双线双接入点模式（推荐）

模式介绍

描述：双线双接入点模式中，用户 IDC 分别通过一条物理专线，与同地域两个腾讯云接入点相连，再连接至腾讯云 VPC。

使用场景：适用于对关键业务可用性和弹性较高的场景。

成本：中。



容灾说明

双线双接入点模式的专线网络架构在各类故障场景下对业务的影响如下。

故障类型	业务影响	恢复措施
物理专线故障	若每条物理专线使用率小于等于 50%，则物理专线负载率骤增，业务不会中断。 若每条物理专线使用率大于 50%，则物理专线负载满载，部分业务数据丢失，业务不会中断。	若业务数据丢失，则需重新申请专线，恢复时长约2~3个月。
网络设备故障	若每条物理专线使用率小于等于 50%，则物理专线负载率骤增，业务不会中断。 若每条物理专线使用率大于 50%，则物理专线负载满载，部分业务数据丢失，业务不会中断。	若业务数据丢失，则需检查并修复网络设备，恢复时间视具体故障而定。
端口异常/光模块故障	若每条物理专线使用率小于等于 50%，则物理专线负载率骤增，业务不会中断。 若每条物理专线使用率大于 50%，则物理专线负载满载，部分业务数据丢失，业务不会中断。	若业务数据丢失，则需检查并修复端口/光模块故障，恢复时间视具体故障而定。
接入点机房故障	若每条物理专线使用率小于等于 50%，则物理专线负载率骤增，业务不会中断。 若每条物理专线使用率大于 50%，则物理专线负载满载，部分业务数据丢失，业务不会中断。	若业务数据丢失，可采取措施如下： 联系接入点机房运营商修复机房故障，恢复时间视具体故障而定。 重新申请专线连接至其他接入点，恢复时长约 2-3 个月。

双线单接入点模式

模式介绍

描述：双线单接入点模式中，用户 IDC 通过两条物理专线与一个腾讯云接入点连接，再连接至腾讯云 VPC。
使用场景：适用于非关键业务场景，例如云上开发和测试环境。
成本：中。

容灾说明

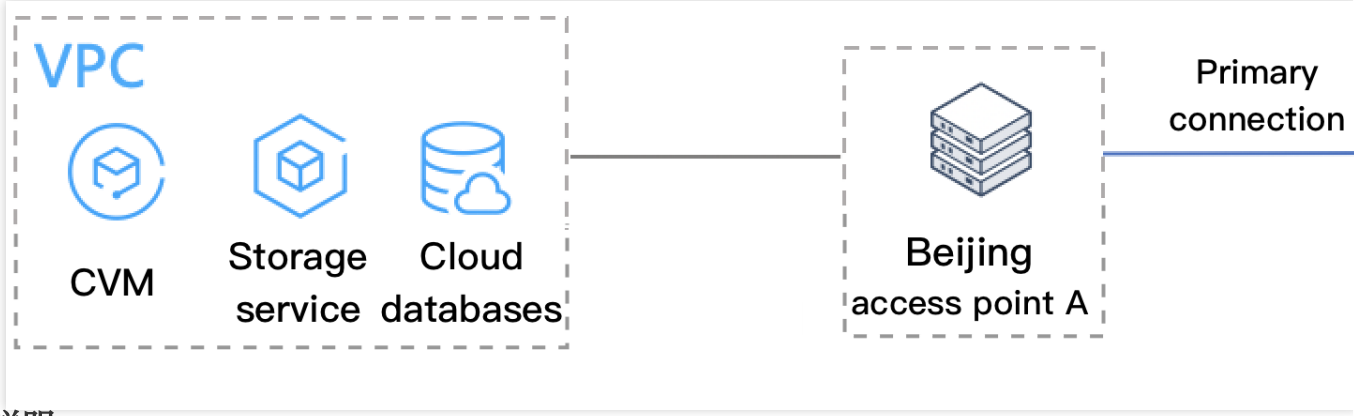
双线单接入点模式的专线网络架构在各类故障场景下对业务的影响如下。

故障类型	业务影响	恢复措施
物理专线故障	若每条物理专线使用率小于等于 50%，则物理专线负载率骤增，业务不会中断。 若每条物理专线使用率大于 50%，则物理专线负载满载，部分业务数据丢失，业务不会中断。	若业务数据丢失，则需重新申请专线，恢复时长约2~3个月。
网络设备故障	业务中断	排查、修复网络设备故障，恢复时间视具体故障而定。
端口异常/光模块故障	业务中断	排查、修复本地端口/光模块故障，恢复时间视具体故障而定。
接入点机房故障	业务中断	联系接入点机房运营商修复机房故障，恢复时间视具体故障而定。 重新申请专线连接至其他接入点，恢复时长约 2-3 个月。

单线单接入点模式

模式介绍

描述：单线单接入点模式中，用户 IDC 通过一条物理专线与一个腾讯云接入点相连，再连接至腾讯云 VPC。
使用场景：适用于不需要高弹性和高可用性的非关键业务场景。
成本：中。



容灾说明

单线单接入点模式的专线网络架构在各类故障场景下对业务的影响如下。

故障类型	业务影响	恢复措施
物理专线故障	业务中断	重新申请专线，恢复时长约 2-3 个月。
网络设备故障	业务中断	排查、修复网络设备故障，恢复时间视具体故障而定。
端口异常/光模块故障	业务中断	排查、修复本地端口/光模块故障，恢复时间视具体故障而定。
接入点机房故障	业务中断	联系接入点机房运营商修复机房故障，恢复时间视具体故障而定。 重新申请专线连接至其他接入点，恢复时长约 2-3 个月。