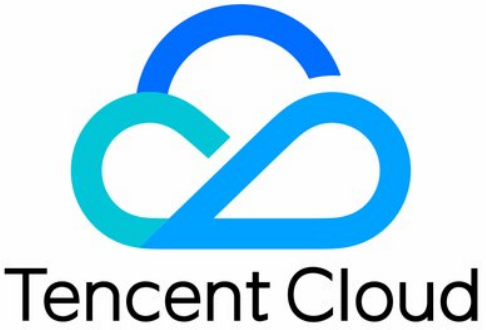
VPN 连接

产品简介



Copyright Notice

Trademark Notice

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

产品简介
产品概述

Last updated：2024-07-02 15:07:31

VPN 连接（VPN Connections）是指在 Internet 公共网络上建立的一个安全的网络连接，通过加密通道方式将企业数据中心（IDC）、内部办公网络与腾讯云的私有网络 VPC 安全的连接起来。

> **说明：**
> 腾讯云 VPN 连接在国家相关政策法规下提供服务，不提供访问 Internet 功能，禁止通过技术方式绕过网络审查访问境外网络，不提供代理功能。

腾讯云 VPN 支持 IPsec 和 SSL 网络安全协议，后文中我们将使用 IPsec 协议的 VPN 连接简称为 IPsec VPN，使用 SSL 协议的 VPN 连接，简称为 SSL VPN。
腾讯云 IPSec VPN 支持通过公网和私网访问云上资源，后文中我们将通过公网访问云上资源的 VPN 连接简称为公网 VPN，通过私网访问云上资源简称为私网 VPN。

> **说明：**
> 如需使用私网类型的 VPN，请 提交工单 进行咨询。

观看视频

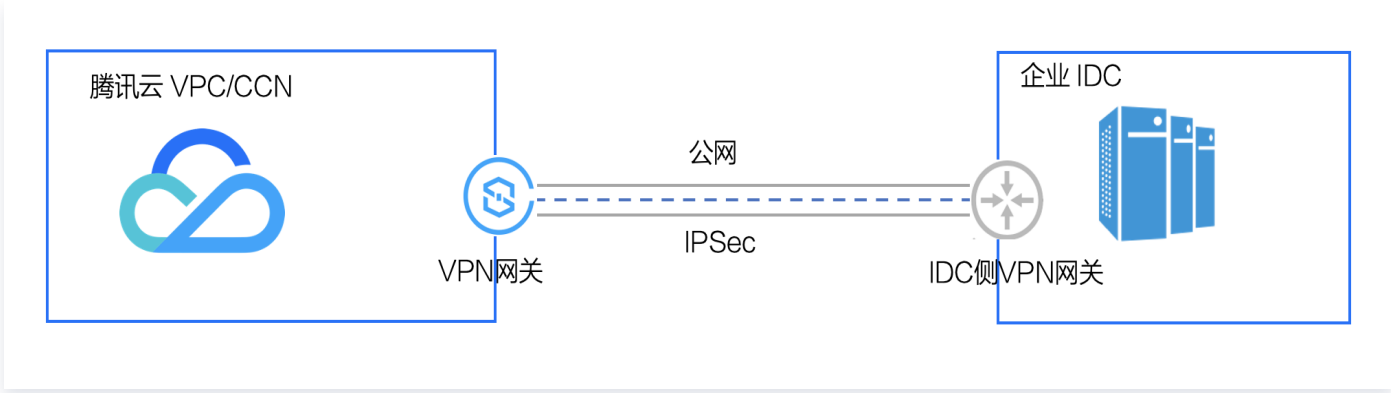
IPSec VPN

腾讯云 VPN 连接分为如下组成部分：

- VPN 网关：创建的 IPsec VPN 网关。
  - VPC 型 VPN 网关：当您需要与单个 VPC 通信时，可通过 VPC 型 VPN 网关接入 VPC。
  - CCN 型 VPN 网关：当您需要与多个 VPC 通信时，可通过 CCN 型 VPN 网关接入云联网，实现全流量互通。

    > **说明**
    > 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。
- 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）。

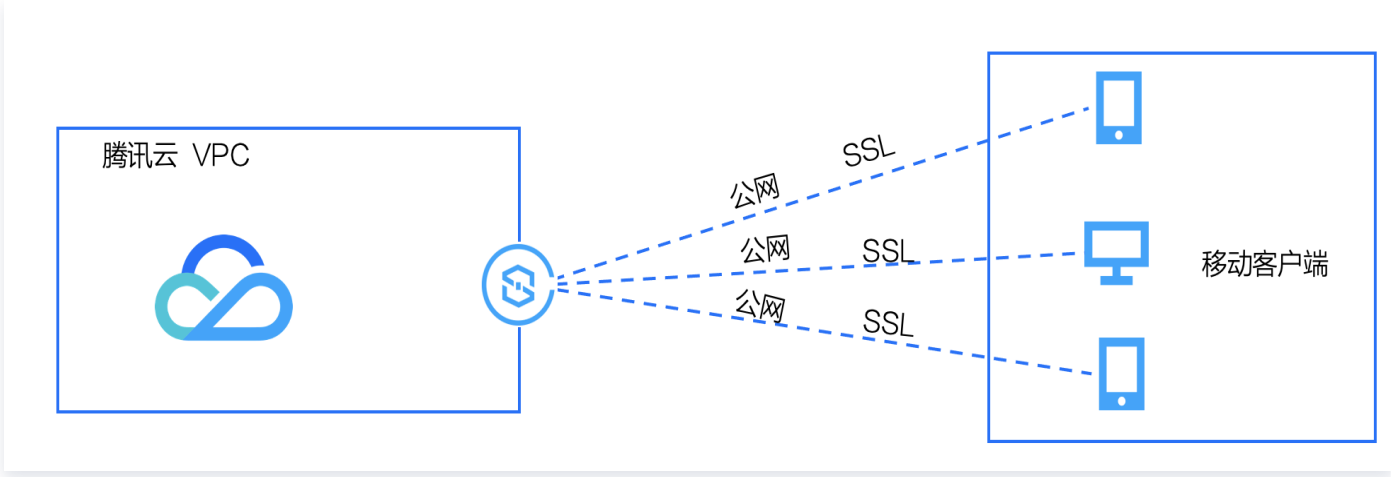
- VPN 通道：加密的 IPsec VPN 通道。



SSL VPN

腾讯云 SSL VPN 连接分为如下组成部分：

- SSL VPN 网关：创建的 SSL 协议类型的 VPN 网关。
- SSL 服务端：提供 SSL 服务的服务模块，实现数据包的封装与解封装，约定通信端口、加密算法、双方联通网段。
- SSL 客户端：用户移动设备上部署的 VPN 客户端在腾讯云的逻辑实例对象。



产品组成

Last updated：2024-04-19 14:46:21

腾讯云 VPN 支持 IPSec协议 和 SSL协议 两种虚拟网络连接，打通 IDC 、内部办公网络、移动端和腾讯云私有网络 VPC/云联网 CCN 全连接。

IPSec VPN

IPSec VPN 网关

IPSec VPN 网关是 VPC 或云联网建立 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，主要用于腾讯云 VPC 或云联网和外部 IDC 之间建立安全可靠的加密网络通信。腾讯云 VPN 网关通过软件虚拟化处理，采用双机热备策略，单台故障时秒级自动切换，不影响业务正常运行。
VPN 网关带宽上限分为9种：5Mbps、10Mbps、20Mbps、50Mbps、100Mbps、200Mbps、500Mbps、1000Mbps、3000Mbps。
如果您需要 DDoS 高防包 为 VPN 网关提供超大带宽的 DDoS 和 CC 防护，您可以将高防包绑定到 VPN 网关上，实现安全防护。

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），需与腾讯云 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 或云联网与外部 IDC 之间加密通信的 VPN 通道。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 通道不仅支持如目的路由和 SPD 策略的静态路由方式通信，同时也支持动态 BGP 路由通信。
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 或云联网，更多详情，请参见 专线接入服务 。

SSL VPN

SSL VPN 网关

SSL VPN 网关是 VPC 建立 SSL VPN 连接的出口网关 ，与 SSL 客户端（客户移动端）配合使用，主要用于腾讯云 VPC 和客户移动端建立安全可靠的加密网络通信。
如果您需要 DDoS 高防包 为 VPN 网关提供超大带宽的 DDoS 和 CC 防护，您可以将高防包绑定到 VPN 网关上，实现安全防护。

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。从而需要在 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，更多详情请参见 创建 SSL 服务端 。

SSL 客户端

SSL客户端提供移动端连接上服务端的证书，通过双向认证客户端才能与服务端建立通信连接。
支持批量构建、批量证书启停等管理和固定私网 IP。

应用场景

Last updated：2024-05-07 15:43:51

腾讯云 VPN 连接是一款基于 Internet 的远程网络连接服务，VPN 网关是 VPN 连接的重要功能载体，通过加密通道（IPSec、SSL）实现与客户 IDC 、客户移动端、内部办公网络建立安全的网络通道 ，从而实现站点到站点的安全访问，VPN 配置灵活，可满足多种用户通信场景。

IPSec VPN 应用场景

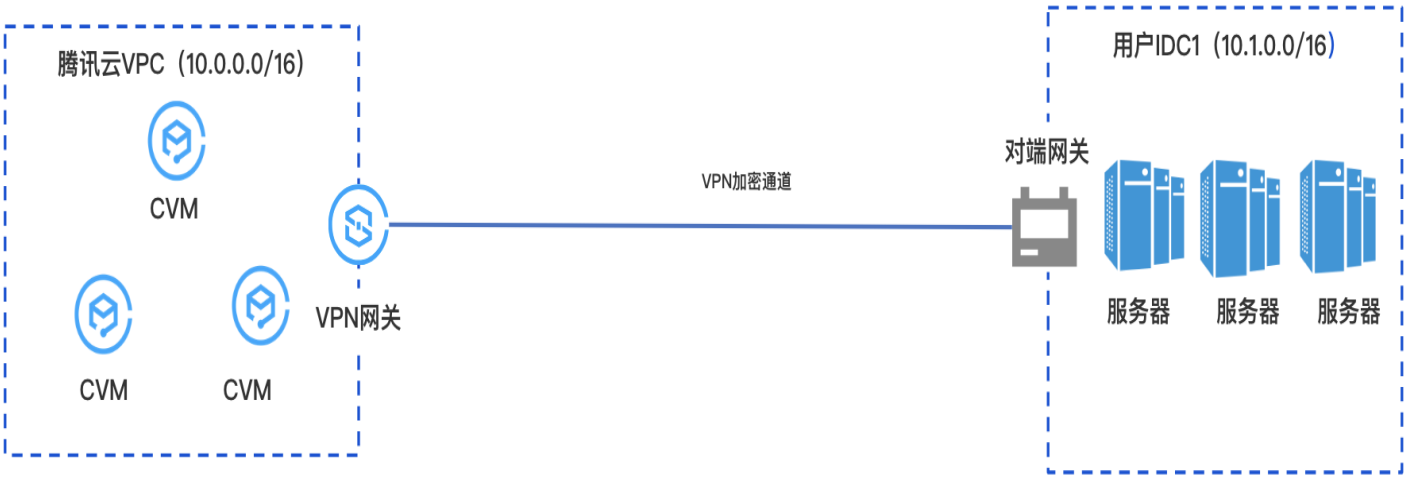
VPN 在进行路由转发时有两种方式：

- 基于 SPD 策略路由，匹配数据流的源网段、目的网段，按照设定好的转发策略进行转发，该方式无法实现路由选路，因此无法中转流量，但可实现场景一、四、六的通信。
- 通过配置 VPN 路由表，使得数据包基于目的网段进行选路转发，该方式即为目的路由方式。利用该功能可实现如下所有场景的通信，其中场景六需要和 SPD 策略路由配合使用，也可以直接使用 SPD 策略路由实现。

> **说明**
> 图中“对端网关”为记录 IDC 侧 IPsec VPN 设备公网 IP 地址的逻辑对象，与 IDC 侧的 IPsec VPN 设备一一对应。

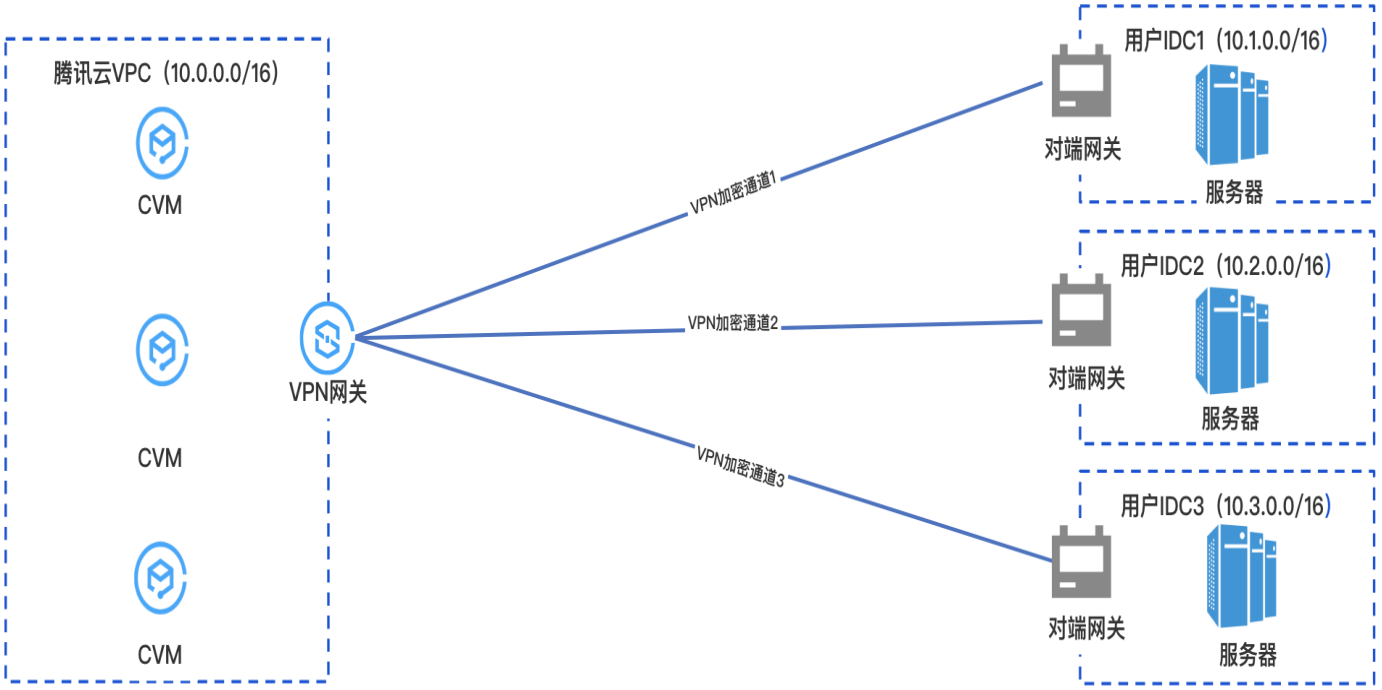
场景一：VPC 与 IDC 通信

VPN 连接实现 VPC 与 IDC 的互访通信。



场景二：单 VPC 与多 IDC 实现全流量互通

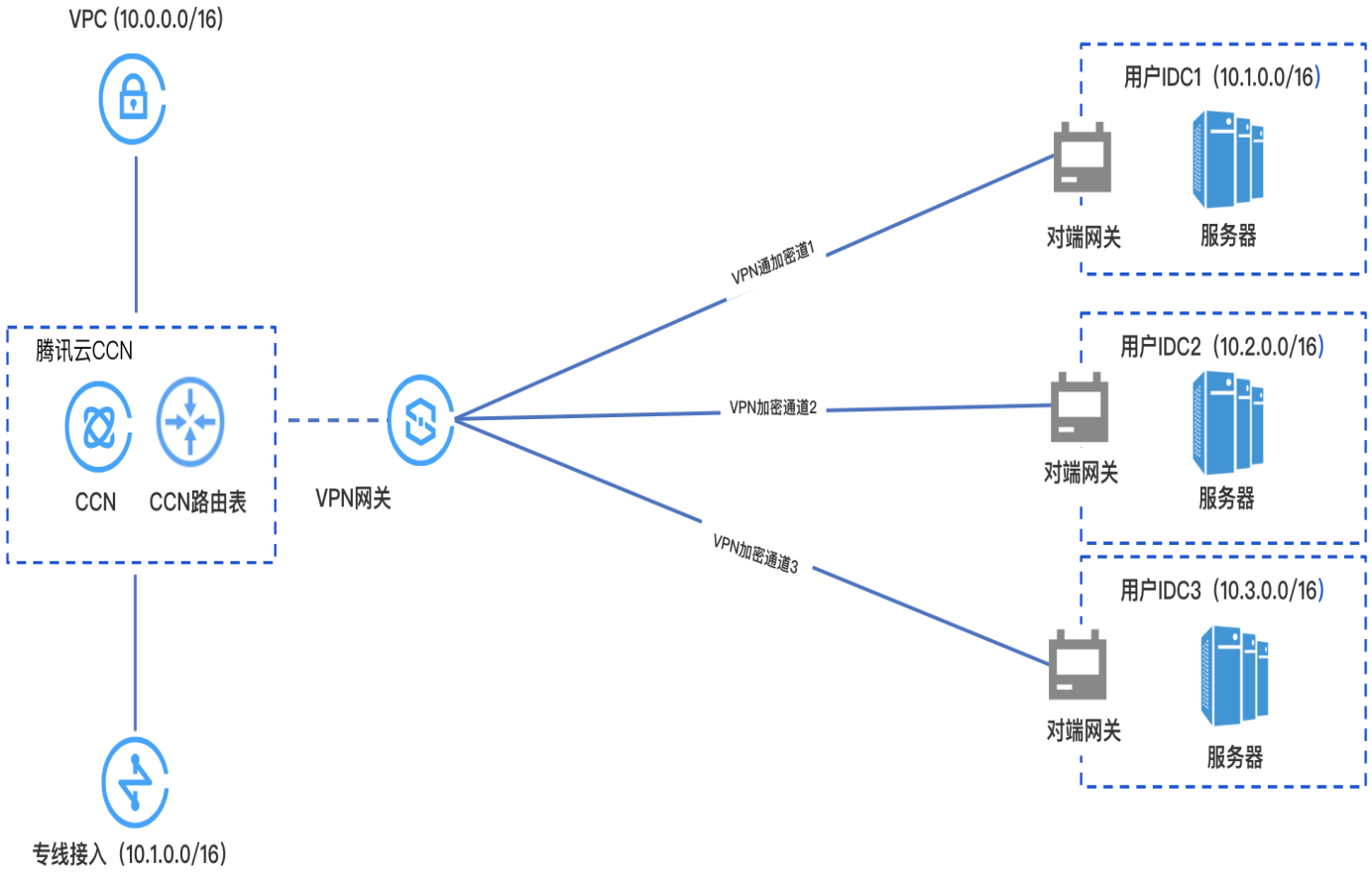
多个 IDC 在通过 VPN 连接上云场景中实现互通。
场景描述：用户 IDC-1、IDC-2、IDC-3 分别通过各自的 IPsec VPN 设备接入腾讯云 VPC 型 VPN 网关，IDC-1、IDC-2、IDC-3 间不仅可以访问 VPN 网关所属私有网络内的各类资源，还可以通过腾讯云 VPN 网关实现中转互通，最终实现 IDC1、IDC2、IDC3 与 VPC 之间的安全通信。



场景三：多 IDC 通过 VPN 网关实现中转通信

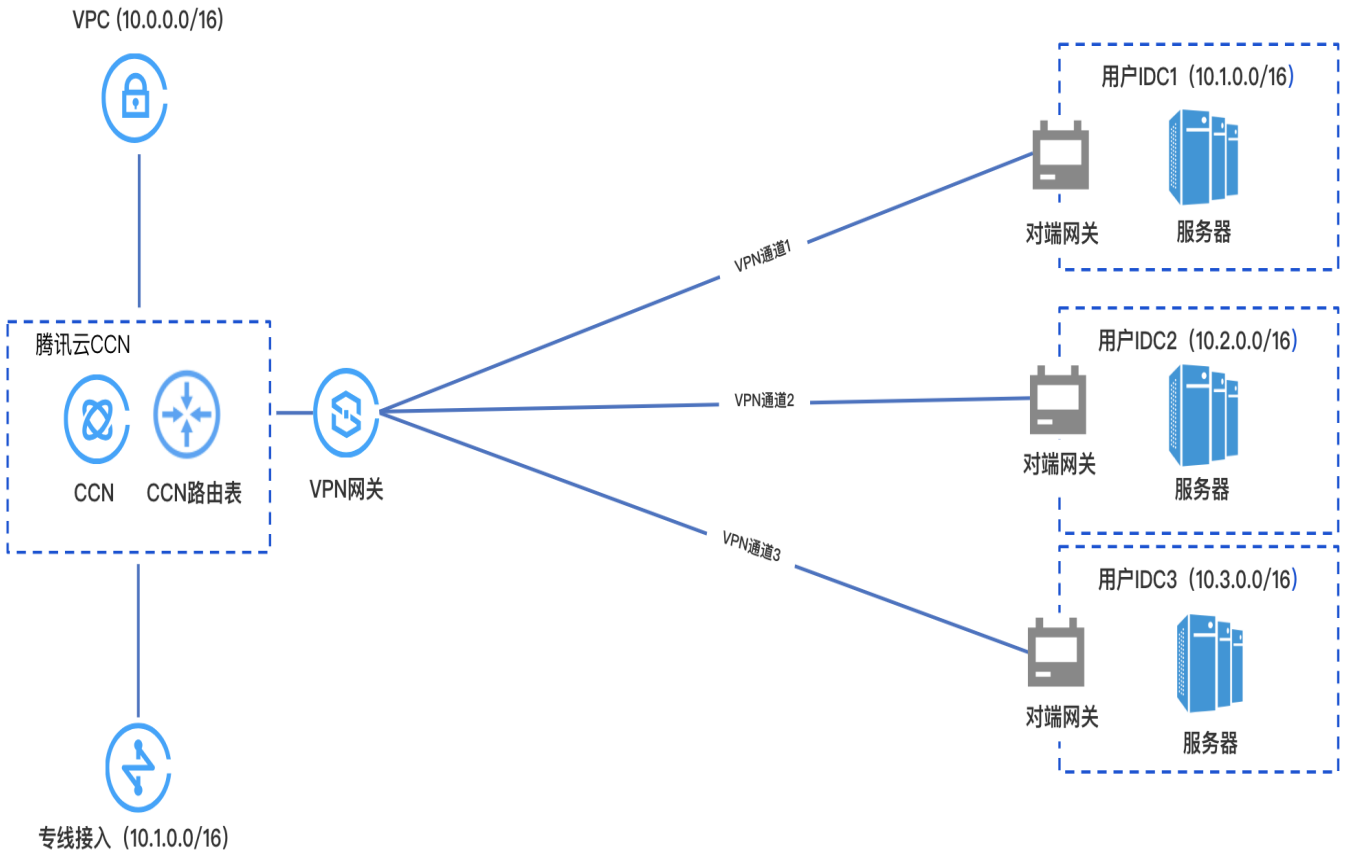
当多个 IDC 需要互通通信，但不需要访问云上资源时，可通过云联网型 VPN 实现中转互通。

场景描述：用户 IDC-1、IDC-2、IDC-3 分别通过各自的 IPsec VPN 设备接入腾讯云 CCN 型 VPN 网关，IDC-1、IDC-2、IDC-3 之间仅通过腾讯云 VPN 网关实现中转互通，但不需要访问腾讯云公有云资源，该场景下，用户可以创建 CCN 型 VPN 网关，但并不关联至云联网，直接在 VPN 网关实现流量互转。



场景四：多 IDC 与云上多网络实现全流量互通

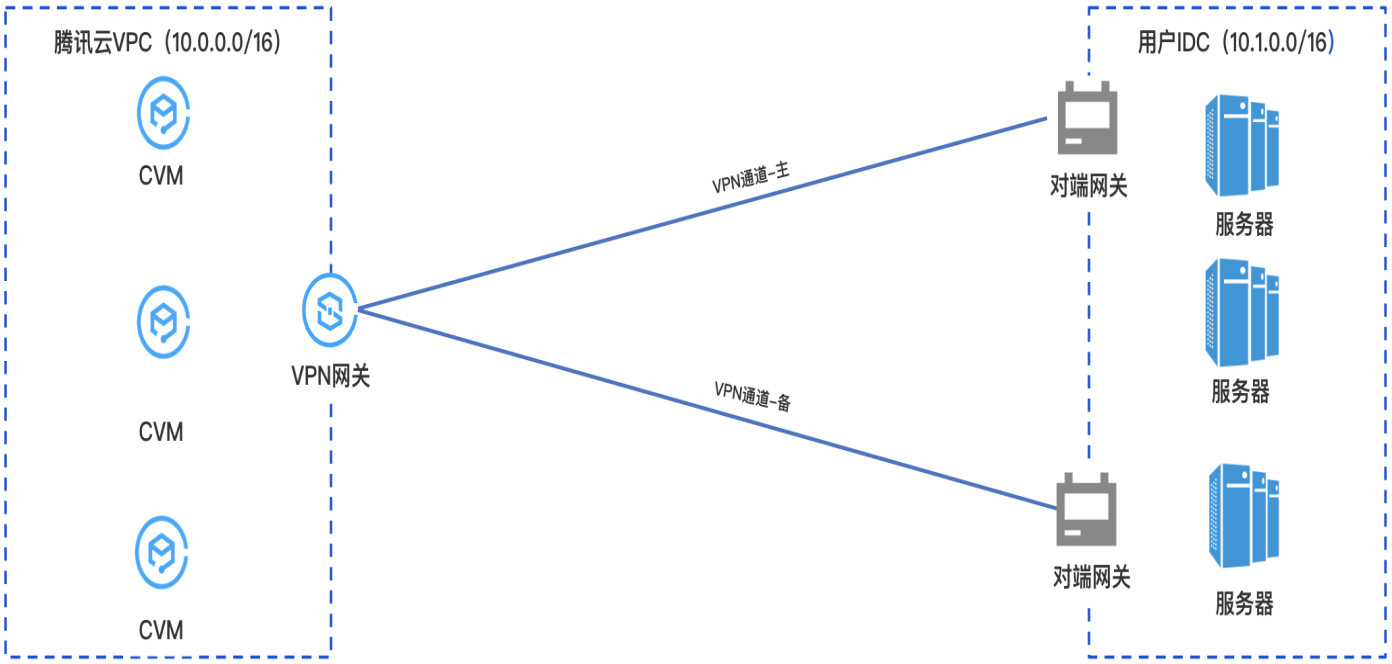
场景描述：用户 IDC-1、IDC-2、IDC-3 分别通过各自 IPsec VPN 设备接入腾讯云 CCN 型 VPN 网关，IDC-1、IDC-2、IDC-3 之间可以通过腾讯云 VPN 网关实现中转互通，同时需要通过云联网访问云联网所关联的 VPC 以及专线网络，该场景下，用户可以创建 CCN 型 VPN 网关，并关联至云联网，实现全流量互通。



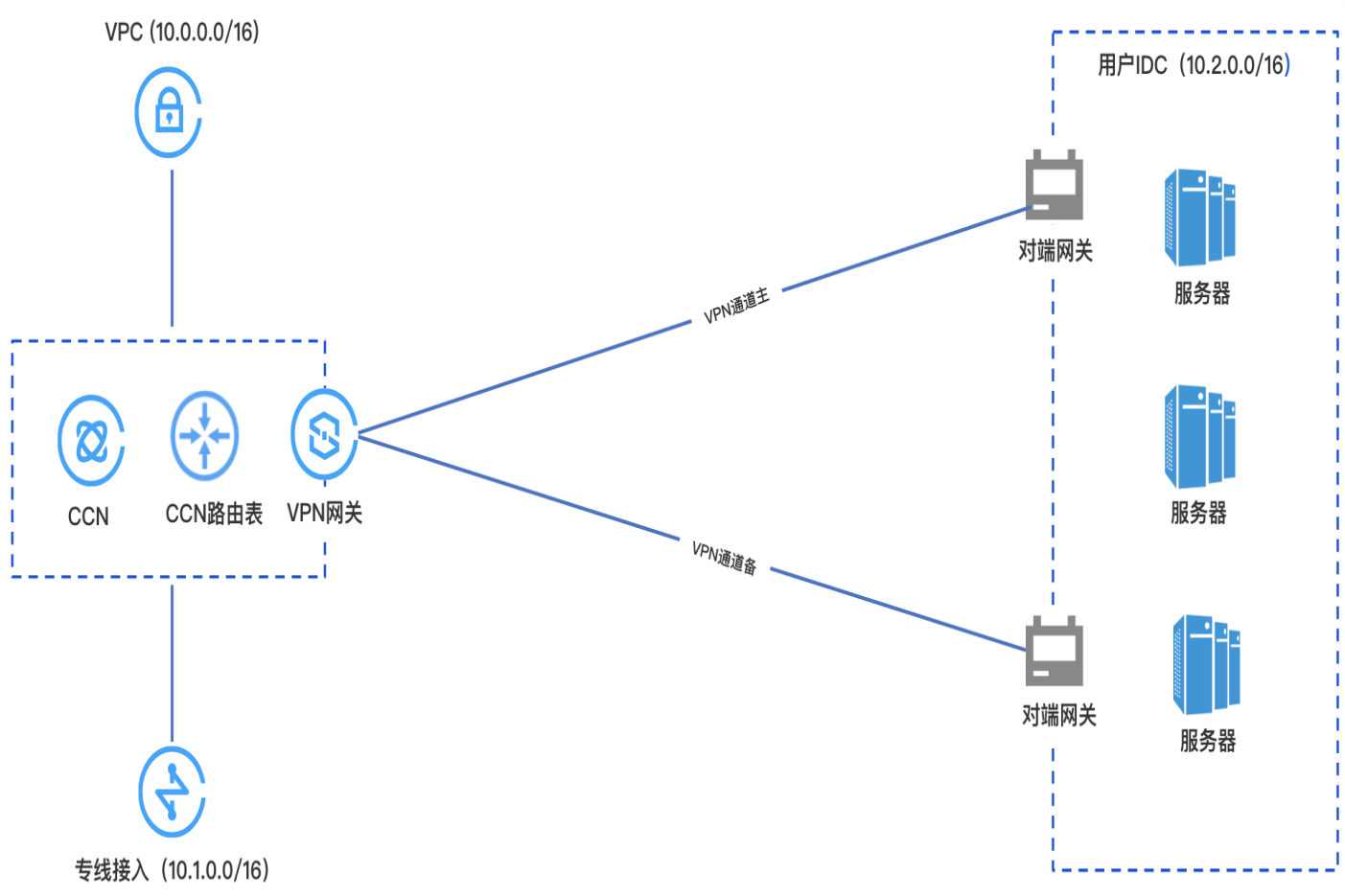
场景五：IDC 通过 VPN 主备通道实现主备容灾上云

当用户 IDC 通过主备 VPN 通道上云，且主通道发生故障时，业务将自动切换到备用通道上，保证了业务的持续性、从而提高业务可靠性。

场景描述一：用户 IDC 仅需要与单个腾讯云 VPC 实现互通，在用户 IDC 侧，用户可以部署两台 IPsec VPN 设备，分别与腾讯云私有网络型 VPN 建立 IPSec VPN 通道，VPN 网关路由表配置两条目的端一致的路由，通过优先级控制，实现主备通道效果；在发生故障时，可以实现路由自动切换。



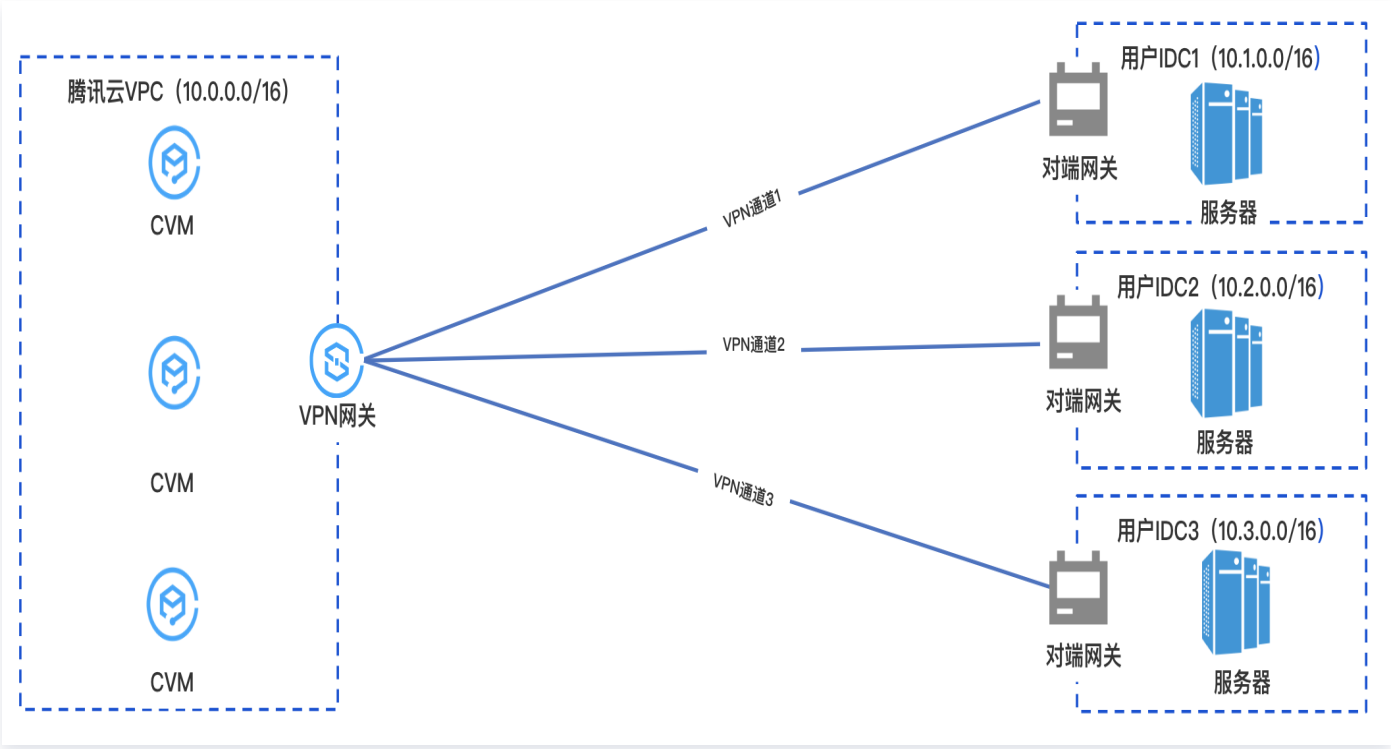
场景描述二：用户 IDC 需要与多个腾讯云 VPC（相同地域或不同地域）以及专线网络实现互通，在用户 IDC 侧，用户可以部署两台 IPsec VPN 设备，分别与腾讯云云联网型 VPN 网关建立 IPSec 通道，VPN 网关路由表可配置两条目的端一致的路由，通过优先级控制，实现主备通道效果；在发生故障时，可以实现路由自动切换。



场景六：单 VPC 通过多条 VPN 通道分别与多个 IDC 通信

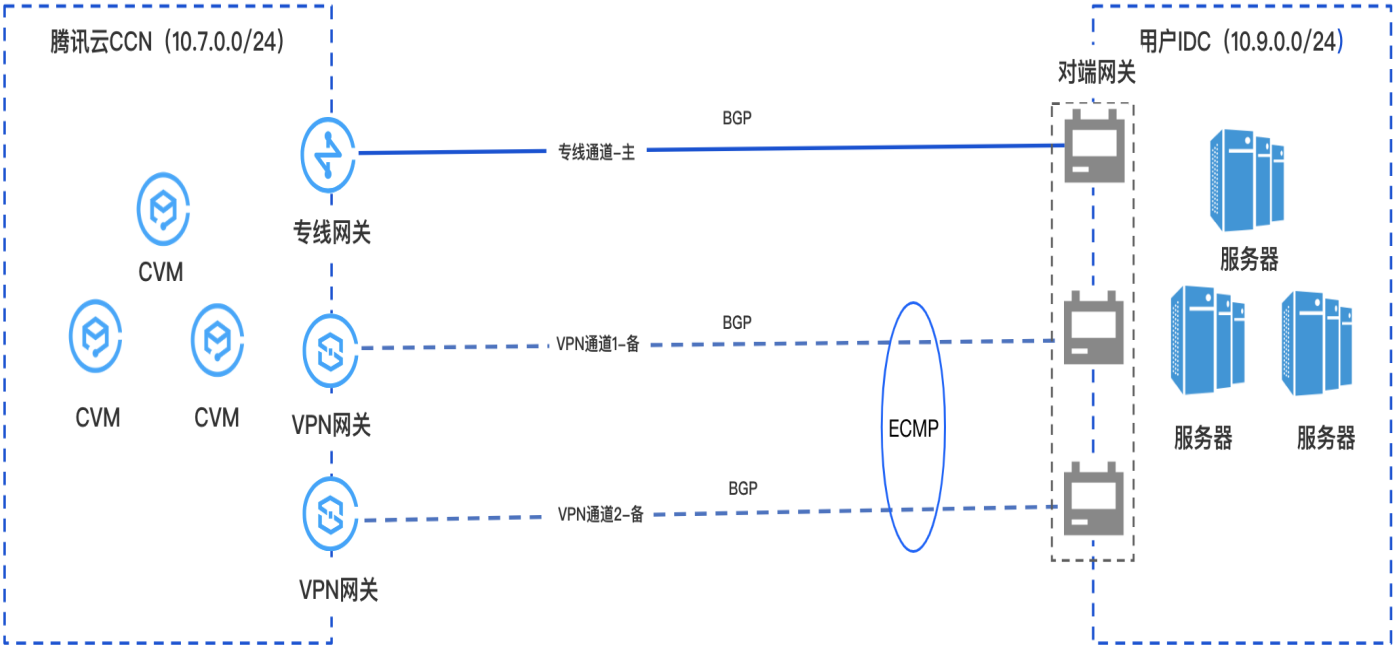
该通信场景与场景二类似，区别在于该场景仅需实现 IDC1 与 VPC 通信、IDC2 与 VPC 通信，IDC3 与 VPC 通信，而 IDC1、IDC2、IDC3 之间无需通信。

- 该场景建议优先使用 SPD 策略路由的方式，分别创建 VPC > IDC1、VPC > IDC2、VPC > IDC3 的规则即可。
- 如果仅使用目的路由的方式，会导致 IDC1、IDC2 与 IDC3 也能互相通信，不符合通信场景，可以在 SPD 策略路由中配置 VPC > IDC1、VPC > IDC2 的规则，再在路由表中配置目的网段为 IDC3 的路由策略，由于 SPD 策略路由的优先级高于目的路由，因此也可实现该场景通信。



场景七：VPN 网关与专线网关实现主备容灾

该通信场景与场景五类似，区别在于该场景使用动态 BGP 进行专线主 + VPN 备实现主备容灾，其中两个 VPN 网关为 ECMP 关系。正常情况下业务流量在专用通道中，当发生故障时自动将流量切至 VPN，恢复正常后业务流量自动切回专线。

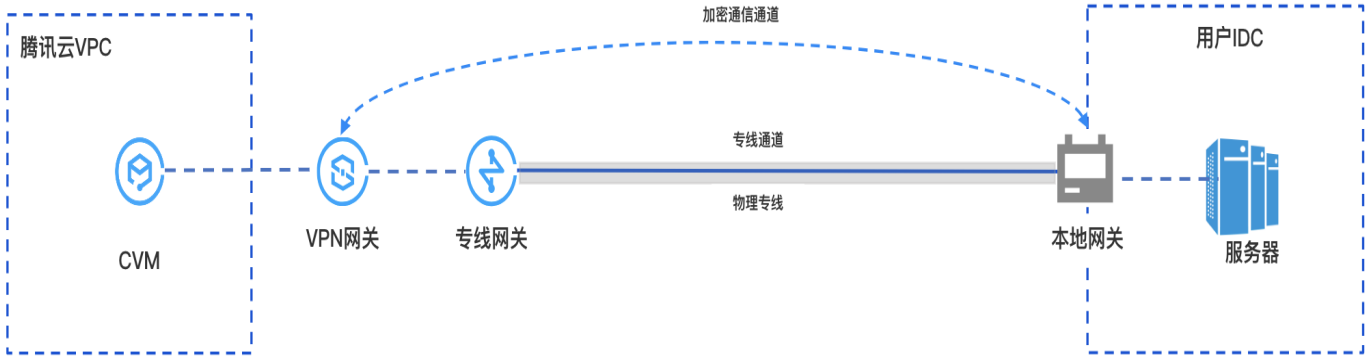


场景八：VPN 网关与专线网关实现私网流量加密通信

在本地数据中心 IDC 通过物理专线和云上 VPC 实现私网通信后，私网 VPN 网关可通过已建立的私网连接与本地网关设备建立加密通信通道。您可以通过相关路由配置引导本地 IDC 和 VPC 要互通的流量进入加密通信通道，实现私网流量加密通信。

说明：

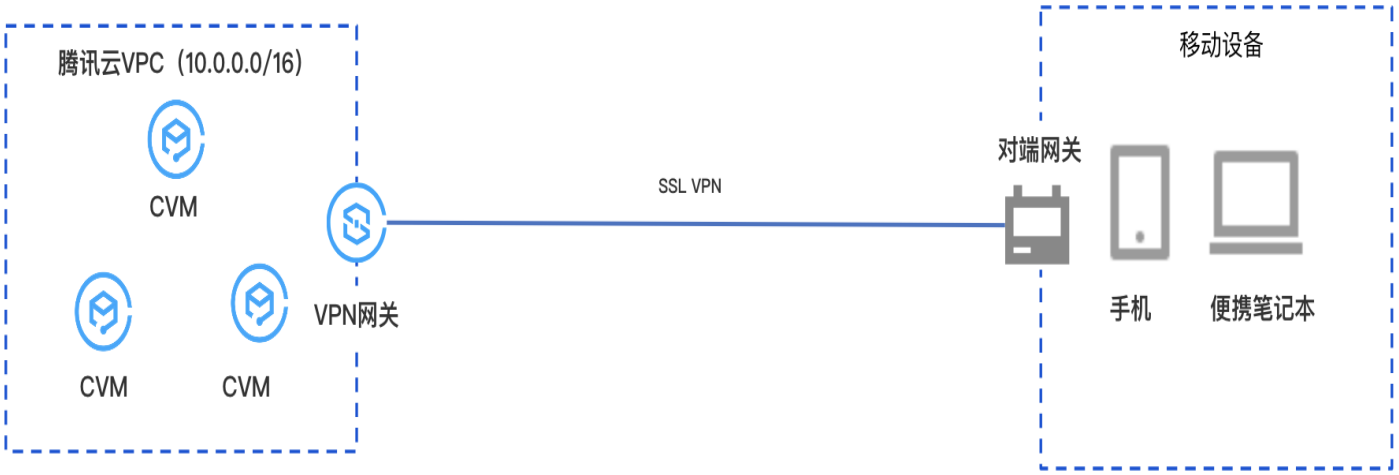
- 本场景中私网 VPN 网关 IP 地址归属租户 VPC。
- 私网 VPN 目前仅支持 VPC 型 VPN，CCN 型 VPN 暂不支持。



SSL VPN 应用场景

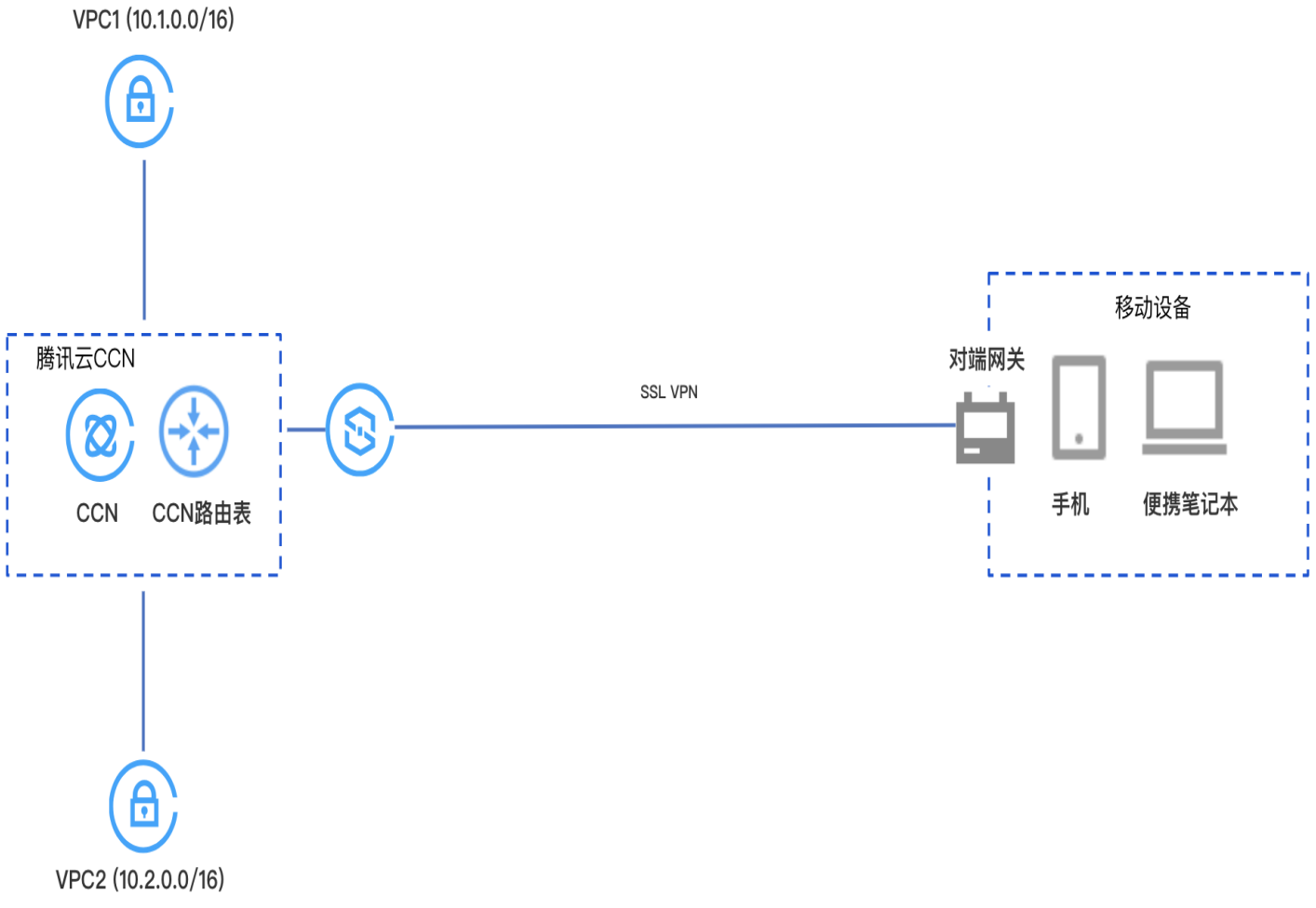
场景1：移动端远程访问单 VPC

用户需要通过 PC 或手机等移动端远程访问自己在云上单 VPC 内资源与服务，可通过 SSL VPN 建立与云上资源的连接。



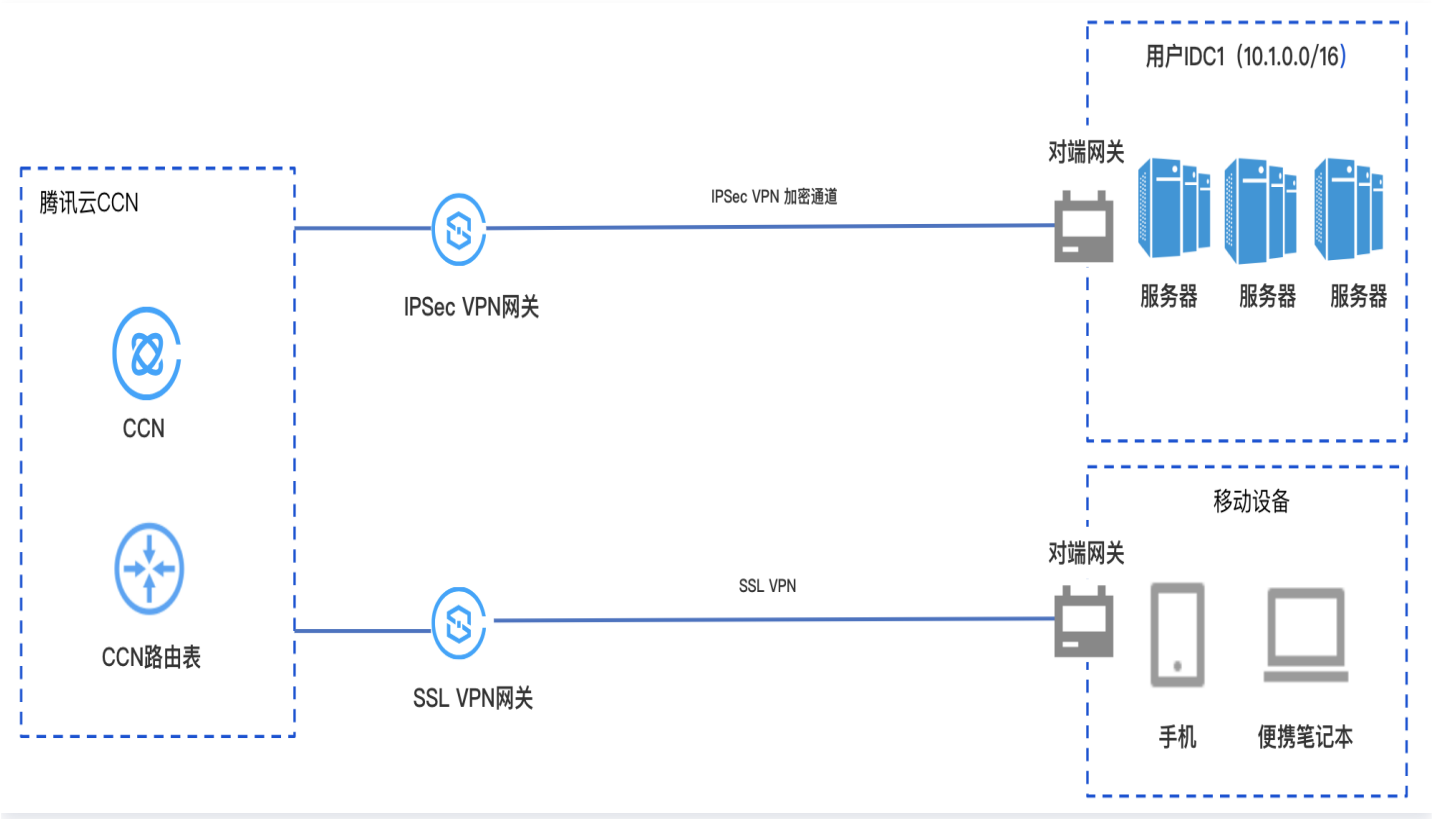
场景2：移动端远程访问多 VPC

用户需要使用 PC 或手机等移动端远程访问自己在云上多个 VPC 内的资源与服务，可通过 CCN 型 SSL VPN 建立与云上资源的连接。



场景3：移动端通过 VPN 访问 IDC 资源

用户通过云联网 CCN 将 IPSec VPN 网关和 SSL VPN 网关关联，用户可以使用 PC 或手机等移动端远程访问自己 IDC 内的资源与服务。



使用限制

Last updated：2024-05-14 16:30:21

VPN 连接

使用 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。
- 如果是1.0的网关，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。
- VPN 连接仅支持 PSK 方式，不支持 CA 认证。
- 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。

VPN 网关

- VPN 是地域级服务，但您可以在任意地域通过互联网连接您的 VPN 网关。
- 不支持指定 VPN 网关的公网 IP 或公网 IP 归属的运营商，不支持 IPv6 地址和 Anycast。
- 腾讯云分配的出入方向带宽与用户购买的带宽相等。
- 目前仅200Mbps、500Mbps、1000Mbps和3000Mbps规格的 4.0 VPN 网关支持动态 BGP。
- 路由优先级：静态路由 > 动态 BGP 路由。
- 私网 VPN：仅 VPC 型的4.0版本 IPSec VPN 支持，如需使用私网类型的 VPN，请 提交工单 进行咨询。

对端网关

- 您必须指定对端网关的 IP 地址，对端网关的公网 IP 不支持如下 IP 地址：
  - 全0、全255或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，如 `1-126.0.0.0` ， `1-126.255.255.255` 。
    - 以 B 类中128-191开头举例，如 `128-191.x.0.0` ， `128-191.x.255.255` 。
    - 以 C 类中192-223开头举例，如 `192-223.x.x.0` ， `192-223.x.x.255` 。
  - 内部服务地址： `169.254.x.x/16` 。
  - IPv6 地址。

- 若通过 IPsec VPN 实现两个 VPC 内的资源互访，两个 VPC 互为对方的对端网关，VPC 网段不应重叠。

SSL 服务端

- 服务端仅支持 UDP，不支持 TCP。
- 修改端口、认证、加密算法等，您需要重新下载客户端配置。
- 客户端网段与本端网段不能重叠。
- SSO 认证
  - VPN3.1版本：身份认证依赖 EIAM 应用，不支持直接对接其他 IdP（Identity Provider）认证。您可以通过 EIAM 服务实现与您企业的认证源对接，也可以选择 EIAM 支持的认证方式，如短信、企微、AD 等。目前身份认证灰度开放，如需使用，请提交 工单申请 。
  - VPN4.0版本：身份认证依赖 CAM 身份角色 配置，支持基于 SAML2.0 的主流第三方 IdP。
- 开启身份认证情况下，您可以使用访问控制。

SSL客户端

- 客户端需要您自行准备，腾讯云 SSL VPN 支持开源 OpenVPN 客户端或兼容的其他商业客户端。
- 每个客户端只能使用一个 SSL 客户端配置证书，暂不支持多台设备使用同一份证书。
- 支持的 OpenVPN 版本：2.4.8及以上的2.x系列，3.x版本。
- 身份认证仅3.x版本 OpenVPN 或兼容的其他客户端支持。
- 在 Windows 系统下，如果您的客户端 OpenVPN 是3.4.0及以上版本，那么 SSL 服务端配置时需要配置加密和认证算法，其中认证算法仅支持 SHA1。
- 单次最多可批量创建100个 SSL 客户端。

资源限制

IPsec VPN 限制

> **说明：**
> 私网 VPN 网关暂不支持动态 BGP 路由。

资源	VPN限制
每个账号每个地域内 VPC 型 IPsec VPN 网关数	10
每个账号每个地域内云联网型 IPsec VPN 网关数	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	20 **说明：** • 同一个对端网关支持的 VPN 通道数为账户级配额。 • 同一个对端网关与同一个 VPN 网关仅可建立一个 VPN 通道。
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
每个 VPN 网关路由表支持的路由条目	1000
新增路由页面一次支持最多增加的路由条目	10
每个 VPN 网关支持的动态 BGP 学习到路由条目	500
每个 VPN 通道动态 BGP 发送的路由条目	10000
BGP ASN	默认64551，取值范围为1 – 4294967295，其中139341、45090、58835不可用。

SSL VPN 限制

资源	限制（个）
每个账号每个地域内 VPC 型 SSL VPN 网关数	10
一个 SSL VPN 网关支持创建的 SSL 服务端的个数	1
一个 SSL 服务端支持添加的本端网段个数	5
一个 SSL 服务端支持添加的客户端网段个数	1 **说明：**

	为保证您的客户端均能分配到 IP 地址，建议您指定的客户端网段所包含的 IP 地址个数大于 SSL VPN 连接数。
SSL 客户端证书的有效期	3年
SSL 连接数限制	• [5,100]Mbps SSL VPN 网关最大支持100个 SSL 连接数。 • 200/500Mbps SSL VPN 网关最大支持500个 SSL 连接数。 • 1000Mbps SSL VPN 网关最大支持1000个 SSL 连接数。 **说明：** • SSL 连接数为连接客户端的数量，SSL 连接数配置后暂不支持修改，配置时请提前做好规划。 • SSL VPN 网关可连接的客户端数还与您创建时配置的 SSL 连接数相关。例如，创建时您设置了5个连接数，那么该网关最大可以连接客户端数为5个。

相关产品

Last updated：2024-04-19 14:46:21

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。
DDoS 高防包	可将 DDoS 高防包绑定到 VPN 网关上，实现超大带宽的 DDoS 和 CC 安全防护。
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 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。
云联网	云联网型 VPN 网关可以关联至云联网，实现 IDC 与云联网间的加密通信。