

私有网络

产品简介

产品文档



腾讯云

【版权声明】

©2013-2018 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

产品简介

产品概述

主要功能

产品优势

应用场景

使用限制

词汇表

典型部署方案

内外网隔离的公有云部署

多层Web 应用的隔离部署

容灾部署

全球同服方案部署

VPN接入的混合云部署

专线接入的混合云部署

基本概念

网关

VPC 内可部署的其它服务

产品简介

产品概述

最近更新时间：2018-06-09 12:26:57

腾讯云私有网络是什么？

腾讯云私有网络（Virtual Private Cloud，VPC）是一块您在腾讯云上自定义的逻辑隔离网络空间，与您在数据中心运行的传统网络相似，托管在腾讯云私有网络内的是您在腾讯云上的服务资源，包括 [云服务器](#)、[负载均衡](#)、[云数据库](#) 等。您可以完全掌握您的私有网络环境，包括自定义网段划分、IP 地址和路由策略等，并通过 [网络 ACL](#) 和 [安全组](#) 等实现多层安全防护。同时，您也可以通过 [IPsec VPN / 专线](#) 连通私有网络与您的数据中心，灵活部署混合云。

为什么选择腾讯云私有网络？

- **无需网络设备采购、简化运维**

在腾讯云私有网络内，您可以通过控制台或 API 自定义网段划分、创建子网、配置路由表和网关等，以软件定义网络，节省设备及运维成本。

- **全球部署、跨账户互通**

通过 [对等连接](#) 服务，您可以在一分钟内互联海内外多地云资源，轻松实现全球同服和两地三中心容灾部署。同时，通过跨账号对等连接，您还可与腾讯云上的其它合作伙伴实现数据互通，快速构建开放式云端生态。

- **高性能、灵活 Internet 访问**

支持 1000 W 并发连接、5 Gbps 带宽的双机热备 [NAT 网关](#) 帮助您轻松打破 Internet 访问性能瓶颈。您还可以通过 [弹性 IP](#) 灵活绑定云资源的服务，轻松配置哪些实例可以访问 Internet。

- **轻松部署混合云**

稳定可靠的 [IPsec VPN / 专线](#) 连接腾讯云私有网络至您的数据中心，您可根据业务量弹性扩展应用程序的云服务器等资源，既降低了企业 IT 运维成本，又不用担心企业核心数据的扩散，轻松构建混合云。

- **安全无死角**

腾讯云私有网络是一个内外网隔离的网络环境，通过 [网络 ACL](#) 和 [安全组](#) 分别从子网和主机维度控制网络流量，可以精确到协议和端口级粒度，多维度、全方位满足您网络安全需求。

选择基础网络 or 私有网络？

腾讯云上的网络分为基础网络和私有网络，其中：

- 基础网络是腾讯云上所有用户的公共网络资源池（如图左所示）。所有 [云服务器](#) 的内网 IP 地址由腾讯云统一分配，配置简单，使用方便，适合对操作易用性要求比较高、需要快速使用云服务器的场景。
- 私有网络是用户在腾讯云上建立的一块逻辑隔离的网络空间（如图右所示）。在私有网络内，用户可以自由定义网段划分、IP 地址和路由策略。与基础网络相比，私有网络更适合有网络自定义配置需求的场景。

私有网络和基础网络的功能区别如下表所示：

功能	私有网络	基础网络
租户关联	基于 GRE 封装的逻辑隔离网络	租户关联
网络自定义	支持	不支持
路由自定义	支持	不支持
自定义IP	支持	不支持
互通规则	支持跨地域跨账号互通	同租户同地域互通
安全控制	安全组 和 网络 ACL	安全组

快速使用

- 了解腾讯云 VPC 时，通常会涉及到一些基本概念，详情请参考 [名词解释](#)。
- 若您第一次使用腾讯云私有网络，需获取有关腾讯云 VPC 的实践介绍，请完成练习 [VPC 快速入门](#)。该练习将指导您完成创建带有子网的 VPC 并在您的子网中启动云服务器实例访问公网。
- 下表列出了您在使用腾讯云 VPC 服务时，可为您提供帮助的相关资源。

资源	说明
VPC 主要功能	VPC 的功能简介
VPC 使用限制	VPC 内服务使用的约束
腾讯云 VPC 文档	API 文档和开发者指南
腾讯云 VPC 购买指导	计费及到期通知等信息

资源	说明
腾讯云 VPC 论坛	社区论坛，用于讨论腾讯云 VPC 的技术性问题。
常见问题	VPC 的常见问题
帮助中心	VPC 的帮助中心
联系我们	我们专业的工程师团队将为您提供 7 * 24 小时不间断的技术服务。

主要功能

最近更新时间：2018-06-09 13:36:28

私有网络 (Virtual Private Cloud) 是一块用户可自定义的逻辑隔离网络空间。在私有网络内，您可以自由定义网段划分、IP 地址和路由策略，部署 [云服务器](#)、[负载均衡](#)、[云数据库](#) 等云服务资源。您在腾讯云上的私有网络不仅可以灵活访问 Internet，而且有丰富的接入方式连接您的数据中心，助力您快速部署混合云。同时，腾讯云私有网络 [对等连接](#) 和 [基础网络互通](#) 功能可以轻松连接内网资源，帮助您轻松实现全球同服和两地三中心容灾。此外，腾讯云私有网络上的 [网络 ACL](#) 和 [安全组](#) 能帮您多维度全方位保证网络安全性。

自定义网络

您可以通过控制台或者 API 自定义私有网络网段、子网网段和路由控制策略，还可以进一步将网络继续划分为多个子网，并在子网内部署应用程序和服务。同时，通过合理设置路由策略，您可以灵活管理 VPC 内、公网和混合云等资源的网络流量转发。

灵活、高性能的 Internet 访问

腾讯云 VPC 为您提供灵活、高性能的 Internet 连接方式，包括弹性 IP、NAT 网关和公网网关。

功能	详述
弹性 IP (EIP)	弹性 IP (Elastic IP , EIP) 是可以独立申请的公网 IP 地址，支持与实例（如：云服务器、NAT 网关）的动态绑定和解绑。 典型应用场景： 1. 保留 IP。国内的 IP 和 DNS 之间需要域名备案。 2. 屏蔽实例故障。例如：动态 DNS 映射把 DNS 名称映射到 IP 地址，传播这个映射变化到整个 Internet 可能需花费 24 小时，而弹性 IP 实现了 IP 从一个云服务器到另一个云服务器的漂移。在任何云服务器出现故障时，只需启动另一个实例并重新映射它，从而快速屏蔽实例故障。

功能	详述
NAT 网关	NAT 网关是私有网络访问 Internet 的一种方式，能在内外网隔离时，将私有网络中内网 IP 地址和公网 IP 地址进行转换。 典型应用场景： 1. 大带宽、高可用公网访问。NAT 网关最大支持 1000 W 并发连接、5 Gbps 带宽和 10 个弹性 IP，双机热备，自动容灾，99.99% 服务可用性。针对需要超大带宽、公网 IP 使用量大、部署服务较多的公网访问应用场景。 2. 安全的公网访问。腾讯云私有网络的 NAT 网关提供 IP 的安全转换。如果您希望隐藏私有网络内主机的公网 IP 以避免暴露其网络部署，同时又希望访问公网，使用腾讯云 NAT 网关即可实现。
公网网关	公网网关是一种云服务器，具备转发 Internet 和私有网络之间流量的功能，没有外网 IP 但需要进行 Internet 访问的云服务器可通过公网网关来访问 Internet。

稳定、可靠的用户数据中心连接

如果您希望构建企业的混合云部署，即连接您的云上计算资源及本地数据中心，那么可以使用公网 VPN / 专线接入连接来实现。

- [VPN 连接](#)

VPN 连接是一种通过公网加密通道连接您 IDC 和腾讯云私有网络的方式。您可以在控制台创建私有网络的 VPN 网关、IDC 侧的对端网关和支持 IPsec 加密协议的 VPN 通道，快速实现私有网络和您本地数据中心的安全通信，助力您快速部署混合云。

- [专线接入](#)

专线接入是一种通过物理专线打通您数据中心和位于多个地域腾讯云计算资源的服务，帮助您建立灵活、可靠的混合云网络连接。专线接入支持双机热备、SLA 服务保障和国内外多地互联，完全满足金融等高质量网络互联要求。

腾讯云上资源灵活互通

您可以通过对等连接和基础网络互通实现私有网络内的资源与其它云资源的互通。

- [对等连接](#)

对等连接是一种连接两个私有网络的服务，使被连接的两个私有网络就像处于同一私有网络，可以帮助您轻松实现全球同服和两地三中心容灾部署。

- [基础网络互通](#)

基础网络互通是指将基础网络内的云服务器关联至指定私有网络的服务，可以打通基础网络中的云服务器与私有网络之间的网络通信，实现内网资源平滑连接。

- 终端连接

终端连接可帮助您实现 VPC 内实例通过内网与基础网络实例通信，其原理是将基础网络实例 IP 与私有网络内 IP 建立映射，访问该私有网络 IP 即访问基础网络实例，支持的基础网络产品包括：LB、CDB、CMEM、REDIS、MongoDB，不支持跨地域 / 跨账号，方向：单向（VPC 访问基础网络），如果有需要，欢迎提交工单申请。

多维度、全方位安全防护

您可以通过网络 ACL 和安全组实现端口和实例维度的资源访问控制。帮助您全方位提高云服务器安全性。

- [网络访问控制列表（Access Control List, ACL）](#)

网络访问控制列表是一个子网级别的无状态可选安全层，可作为防火墙以控制进出子网的数据流，可以精确到协议和端口维度。

- [安全组](#)

安全组是一个实例级别的包过滤功能的虚拟防火墙，它用于设置单台或多台实例的网络访问控制。您可以将同一地域内具有相同网络安全隔离需求的云服务器实例加到同一个安全组内，通过网络策略对云服务器的出入流量进行安全过滤。

产品优势

最近更新时间：2018-06-09 13:23:21

安全隔离

100% 网络逻辑隔离，满足金融政企的安全隔离需要。

访问控制

灵活的访问控制规则，支持基于安全组（防火墙）和网络 ACL 两种级别的访问控制。

灵活部署

- 全自定义网络划分和路由部署，提供可视化网络拓扑图，让您快速掌握私有网络。
- 提供 [对等连接](#) 和 [基础网络互通](#) 功能，让您的私有网络更灵活更高效。

丰富接入

私有网络支持以下连接出口：

- 访问 Internet（主机通过自有公网 IP）。
- 访问 Internet（公网网关转发）。
- 访问 Internet（NAT 网关转发）。
- 访问私有数据中心：VPN 网关（基于公网的 IPsec 加密通道）。
- 访问私有数据中心：专线网关（基于运营商专线的互联）。
- 访问其他私有网络：对等连接（私有网络之间流量访问）。

应用场景

最近更新时间：2018-06-09 13:27:34

托管简单网站

您可以像使用普通网络一样使用私有网络，部署简单的 Web 应用，如博客、网站和日志系统等。通过 [安全组](#) 和 [网络 ACL](#) 等防火墙，您可以使 Web 应用响应 HTTP 等请求，但拒绝 Web 应用访问 Internet，从而保证 Web 应用的安全。在流量突增时，您还可以在 VPC 的中启用 [负载均衡](#) 轻松应对。

相关产品：[云服务器（CVM）](#)、[云数据库](#)、[负载均衡](#)。

托管多层 Web 应用

您可以在私有网络内创建不同子网，整个 Web 层放在一个子网，通过配置 [弹性 IP](#) / [公网网关](#) / [NAT 网关](#) 对外通信，逻辑层单独放在一个子网，只能和 Web 层及数据层通信，数据层放在另外一个子网，只和逻辑层通信，子网和子网之间的流量通过 [网络 ACL](#) 进行控制。腾讯云私有网络可以在给您的应用提供 Internet 服务的同时，又保障数据库服务器的安全，您可以安全灵活地在腾讯云 VPC 中托管多层 Web 应用程序。

相关产品：[云服务器（CVM）](#)、[云数据库](#)、[弹性 IP](#)、[NAT 网关](#)、[公网网关](#)。

弹性混合云部署

您可以在私有网络内部署您的应用程序，在您的企业数据中心部署数据库服务器。腾讯云私有网络提供稳定安全的 [IPsec VPN](#) / [专线](#) 帮您打通企业数据中心与云端资源。您可使用 [弹性伸缩](#) 服务实现根据业务量弹性扩展应用程序的云服务器等资源，既降低了企业 IT 运维成本，又不用担心企业核心数据的扩散，轻松实现弹性混合云部署。

相关产品：[云服务器（CVM）](#)、[云硬盘（CBS）](#)、[弹性伸缩（AS）](#)、[专线接入](#)、[VPN 连接](#)。

使用限制

最近更新时间：2018-06-09 13:35:45

私有网络内基础配额表

资源	限制（个）
同一地域内私有网络个数	5
每个私有网络内的子网数	10
每个私有网络支持关联基础网络主机的个数	100
每个私有网络内的路由表个数	10
每个路由表的路由策略数	50
每个私有网络支持的对等连接数	10
每个私有网络支持的 NAT 网关数	3
每个 NAT 网关支持弹性 IP 个数	10
每个 NAT 网关最多支持转发能力	5 Gbps
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

资源	限制（个）
同一个对端网关支持的 VPN 通道数	10
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
每个私有网络内网络 ACL 数	50
每个网络 ACL 中规则数	入站方向：20 出站方向：20
每个子网关联的网络 ACL 个数	1
每个网络 ACL 关联的子网个数	无限制

专线接入配额表

资源	限制	说明
物理专线 / 用户	10 个	-
专线通道 / 物理专线	10 个	-
专线网关（支持 NAT）/ 私有网络	1 个	-
专线网关（不支持 NAT）/ 私有网络	1 个	-

资源	限制	说明
本端 IP 转换 / 专线网关	100 条	可申请调高配额
对端 IP 转换 / 专线网关	100 条	可申请调高配额
本端源 IP 端口转换 IP 数 / 专线网关	20 个	可申请调高配额
本端目的 IP 端口转换 / 专线网关	100 条	可申请调高配额

词汇表

最近更新时间：2018-06-09 14:08:22

私有网络与子网

术语	英文	说明
地域	Region	地域是腾讯云托管机房分布地区，地域下有不同的可用区。 例如：一个托管机房的地域是北京，可用区是北京一区。处于统一地域的云服务产品可以通过内网互通，不同地域云产品之间内网不互通，选择最靠近您客户的地域，可降低访问时延、提高下载速度。 单击【地域】查看地域选择指南
可用区	Zone	可用区是同一地域下（如广州），电力和网络互相独立的物理区域（一般是一个物理机房），如广州一区，划分可用区的目的是能够保证可用区间的故障隔离（大型灾害故障除外）。 例如，您在可用区一和二部署了同样的业务，可用区一发生电力故障不会影响到可用区二，从而给您提供稳定高可用的服务。 单击【可用区】查看可用区选择指南
私有网络	Virtual Private Cloud	私有网络能帮助您在腾讯云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，但是托管在腾讯云私有网络内的是您在腾讯云上的服务资源，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，腾讯云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，腾讯云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
基础网络	Basic Network	基础网络是腾讯云上所有用户的公共网络资源池，该资源池内云服务器内网 IP 地址由腾讯云统一分配，配置简单，使用方便，适合对操作易用性要求比较高、需要快速使用云服务器的用户，而私有网络更适合有网络管理能力和需求的客户。 查看私有网络和基础网络的区别
子网	Subnet	子网是对私有网络网段的灵活划分，您可以在不同子网内部署应用程序和服务，安全灵活地在腾讯云 VPC 中托管多层 Web 应用程序

术语	英文	说明
CIDR (无类别域间路由)	Classless Inter-Domain Routing	CIDR 由您指定的独立网络空间地址块，通过 IP 和掩码结合，实现对网络的整体划分。以 10.1.0.0/16 为例，斜杠左边为网络块的 IP，斜杠右边为网络块的掩码。通过设定掩码的大小，可以调整网络块的大小设定。网络块包括的 IP 数 = $2^{(32-\text{掩码})}$ ，因而 10.1.0.0/16 网络块最多包含 65536 个 IP 地址。 查看 CIDR 详情
内网 IP	Private IP	内网 IP 是在腾讯云 VPC 或基础网络内分配给实例 IP 地址，内网 IP 地址无法通过 Internet 访问，但可用于 VPC 中或基础网络实例之间的通信
外网 IP	Public IP	外网 IP 地址可通过 Internet 访问，并可用于实例与 Internet 之间或与其他具有公共终端节点的腾讯云资源（如 CDB）之间的通信

路由

术语	英文	说明
路由表	Route Table	路由表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	Routing policy	路由策略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。 查看 路由策略设置详情

访问 Internet

术语	英文	说明
弹性 IP	Elastic IP (EIP)	弹性 IP 是可以独立申请的公网 IP 地址，支持动态绑定和解绑。您可以将其与账户中的云服务器（或 NAT 网关实例）绑定或者解绑，主要作用是： 1. 保留 IP，因为国内的 IP 和 DNS 之间是需要域名备案的。 2. 屏蔽实例故障，例如：动态 DNS 映射把 DNS 名称映射到 IP 地址，传播这个映射变化到整个 Internet 可能需花费 24 小时，而弹性 IP 实现了 IP 从一个云服务器到另一个云服务器的漂移。在任何云服务器出现故障时，只需启动另一个实例并重新映射它，从而快速响应实例故障

术语	英文	说明
公网网关	Public network gateway	公网网关是一种云服务器，具备转发 Internet 和私有网络之间流量的能力，没有外网 IP 但需要进行 Internet 访问的云服务器可通过公网网关来访问 Internet
NAT 网关	NAT gateway	NAT（网络地址转换）网关能在内外网隔离时，将私有网络中内网 IP 地址和公网 IP 地址进行转换，实现私有网络访问 Internet 功能。 NAT 网关支持最大满足 5 Gbps 突增流量和 1000 W 并发连接数，同时作为高可用网关，NAT 网关实现了双机热备，单机出故障自动切换，业务无感知

连接您的数据中心

术语	英文	说明
用户数据中心	Internet Data Center (IDC)	用户数据中心是用户部署在腾讯云外的一整套 IT 设施
Internet 协议安全性	Internet Protocol Security (IPSec)	Internet 协议安全性是一个协议套件，通过验证和加密数据流的每个 IP 数据包来保护 Internet 协议 (IP) 通信安全
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。 腾讯云私有网络 IPsec VPN 接入分为以下几个组成部分： 1. 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。 2. 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。 3. 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，用于私有网络和您的 IDC 之间的加密通信

术语	英文	说明
专线接入	Direct Connect	是一种快速连接腾讯云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腾讯云计算资源，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。 专线接入包括三个组成部分： 1. 物理专线：连接腾讯云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线通道。 2. 专线通道：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线通道实现本地数据中心与多个私有网络的互联。 3. 专线网关：私有网络的专线流量入口，可以接入多个专线通道与多个本地数据中心互联

您在腾讯云上的资源互通

术语	英文	说明
对等连接	Peer connection	对等连接是不同私有网络建立的连接，支持跨账户和跨地域的私有网络之间流量互通。建立了对等连接的私有网络，可以实现 IP 流量互访，两端的云服务器和云数据库等资源可以相互访问
基础网络互通	Classiclink	是腾讯云私有网络与基础网络之间云服务互通。与私有网络连通的基础网络云服务器可通过内网主动访问私有网络内的云服务器、云数据库等计算资源，私有网络内的云服务器也可以通过内网主动访问基础网络云服务器

安全

术语	英文	说明
网络访问控制列表	Access Control List (ACL)	网络访问列表是一个子网级别的无状态可选安全层，可作为防火墙以控制进出子网的数据流，可以精确到协议和端口维度。除此之外，网络 ACL 可以限制网络流量，提高网络性能
安全组	Security Group	安全组是一种有状态的包过滤功能的虚拟防火墙，它用于设置单台或多台云服务器的网络访问控制，可以将同一地域内具有相同网络安全隔离需求的云服务器实例加到同一个安全组内，通过安全组的网络策略对云服务器的出入流量进行安全过滤

典型部署方案

内外网隔离的公有云部署

最近更新时间：2018-06-09 14:28:02

应用场景

用户担心公有云上多租户共享资源池的方式无法保证数据的安全，希望在公有云上使用一个完全隔离的网络环境部署云资源。

用户关注重点：

与其它租户完全隔离，规避多租户共享带来的风险。

解决方案

腾讯云私有网络（Virtual Private Cloud，VPC）是一块您在腾讯云上自定义的逻辑隔离网络空间，与您在数据中心运行的传统网络相似，托管在腾讯云私有网络内的是您在腾讯云上的服务资源，包括云服务器、负载均衡、云数据库等资源。您可以完全掌握您的私有网络环境，包括自定义网段划分、IP 地址和路由策略等，并通过网络 ACL 和安全组等实现多层安全防护。同时，您也可以通过 IPsec VPN / 专线连通私有网络与您的数据中心，灵活部署混合云。

腾讯云上的网络分为私有网络和基础网络，其中：

- **基础网络**

基础网络是腾讯云上所有用户的公共网络资源池（如左图所示）。所有云服务器的内网 IP 地址由腾讯云统一分配，配置简单，使用方便，适合对操作易用性要求比较高、需要快速使用云服务器的场景。

- **私有网络**

私有网络是指用户在腾讯云上建立的一块逻辑隔离的网络空间（如右图所示）。在私有网络内，用户可以自由定义网段划分、IP 地址和路由策略、同样可以部署云服务器和数据库等服务。与基础网络相比，私有网络更适合有网络自定义配置需求的场景。

操作步骤

1. 创建私有网络、初始化子网和路由表。
2. 创建子网。
3. 新建路由表关联子网。

4. 向子网中添加云服务器、数据库等。

详情请参见 [快速入门](#)。

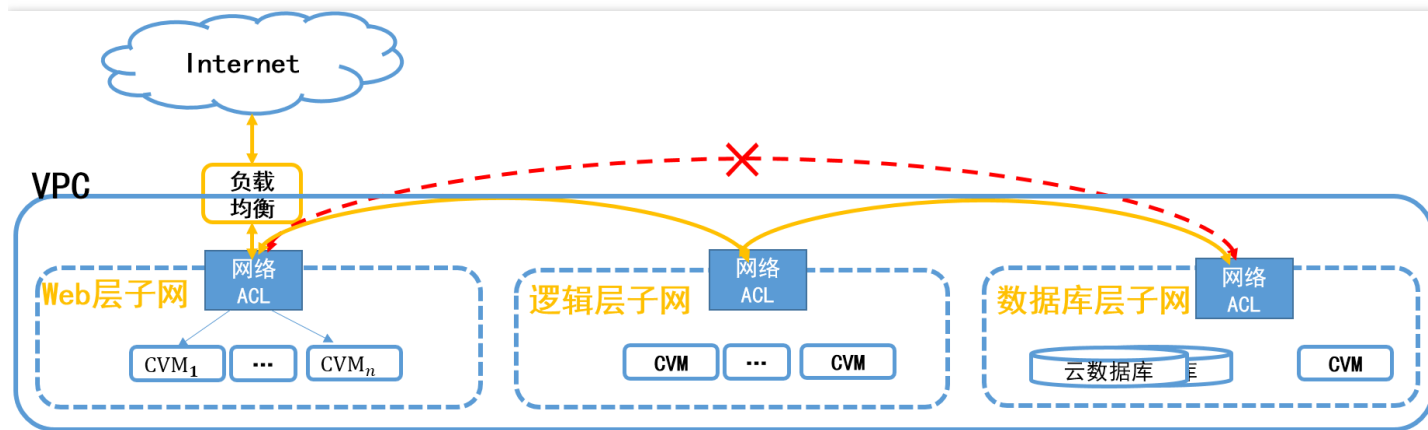
多层Web 应用的隔离部署

最近更新时间：2018-06-09 15:14:17

应用场景

多层 Web 应用的隔离部署，适用于既希望保证 Web 接入层能访问 Internet、响应海量请求的同时，又需要通过网络隔离保障数据库服务器的安全的场景。

您可以在私有网络内创建不同子网，将整个 Web 层放在一个子网，通过配置弹性 IP / 网关云服务器 / NAT 网关与 Internet 通信，使用负载均衡服务将访问流量自动分配到多个 Web 接入层云服务器上；逻辑层单独放在一个子网，只能和 Web 层及数据层通信；数据层放在另外一个子网，只和逻辑层通信，来实现隔离部署。



解决方案

• 私有网络

CIDR(10.0.0.0/16)，并在私有网络内创建三个子网。

• Web 层子网

CIDR(10.0.0.0/24)，将部署了 Web 层应用的云服务器单独放于该子网，该子网可与 Internet 通信以响应用户请求。同时，面对海量请求时，您可以使用负载均衡服务。

• 逻辑层子网

CIDR(10.0.1.0/24)，逻辑层应用所在云服务器单独放于一个子网，以保证逻辑层应用不被公网访问。

• 数据层子网

CIDR(10.0.2.0/24)，为了保证数据的安全，单独分配一个数据子网，在这其中部署数据库产品，只允许逻辑层子网的流量访问。

• 网络 ACL

通过网络 ACL 进行子网间的流量控制。配置规则如“网络 ACL A”和“网络 ACL B”所述。

• 网络 ACL A

绑定逻辑层子网，目标：保证逻辑层应用不被公网访问，能被 Web 层子网和数据库层子网访问，配置规则如下：

◦ 入规则：

协议类型	端口	源 IP	策略	备注
All traffic	ALL	10.0.0.0/24	允许	允许 Web 层访问

◦ 出规则：

协议类型	端口	目的 IP	策略	备注
All traffic	ALL	10.0.0.0/24	允许	允许响应 Web 层访问
All traffic	ALL	10.0.0.0/24	允许	允许访问数据库层子网

• 网络 ACL B

绑定数据库层子网，目标：保证数据库层子网只能被逻辑层子网访问，规则如下：

◦ 入规则：

协议类型	端口	源 IP	策略	备注
All traffic	ALL	10.0.1.0/24	允许	允许逻辑层访问

◦ 出规则：

协议类型	端口	目的 IP	策略	备注
All traffic	ALL	10.0.1.0/24	允许	允许返回逻辑层的请求

操作步骤

为部署多层 Web 应用，您需要完成以下步骤：

1. 创建私有网络，详情请参见 [创建私有网络](#)、[初始化子网和路由表](#)。
2. 创建 Web 层子网，[添加云服务器](#)，部署负载均衡服务，详情请参见 [部署负载均衡实例](#)。
3. 创建逻辑层子网，[添加云服务器](#)。
4. 创建数据层子网，添加云数据库，详情请参见 [购买云数据库](#)。
5. 分别为三个子网配置网络 ACL，配置规则请参见上文 [网络 ACL](#)，操作详情请参见 [快速入门](#)。

容灾部署

最近更新时间：2018-06-09 15:12:20

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，而是从稳定性、可靠性等方向寻求从单中心向多中心化的发展，通过消灭单点，解决单数据中心故障带来的业务风险。

用户关注重点：

- 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（买好的服务器暂时先用）。

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，您可以在另外一个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。流量切换：故障时，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。

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. 通过专线同步本地数据中和云上私有网络中数据中心，详情请参见 [专线操作指南](#)。
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。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，您可以在另一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](#)。

全球同服方案部署

最近更新时间：2018-06-09 16:16:04

应用场景

很多公司基于用户分布情况，将 IT 系统部署在全球不同区域，尤其是游戏公司。

用户关注重点：

- 核心数据集中部署，尽量避免跨区域数据通信。
- 用户分地域就近接入，降低时延。
- 各地域之间数据高速互联，如进行跨服战等。

解决方案

腾讯给出游戏公司全球同服解决方案如下：

• 数据库集中部署

腾讯云数据中心广布全球，现已在全球范围内开通 16 大数据中心，覆盖 5 大洲，游戏数据库中心服可根据业务需要选择部署在腾讯云几大核心机房之一。

选择中心服部署的机房一般可从两个方面入手：

- i. 跟产品运营同学确认游戏希望重点覆盖哪个区域的玩家，如欧美还是东南亚地区等。
- ii. 对比海外各大 IDC 的网络质量和覆盖面，选其最优节点进行部署。

• 多地分区域接入玩家

因全球 200 多个国家到游戏中心服网络时延不一，您可依托腾讯云分布世界各地的 IDC 就近部署一套接入服务，借助 DNSPod 云解析智能调度功能实现玩家的就近访问。另外考虑到大部分时间里玩家主要是和本地域玩家一起游戏，所以玩家数据也可以做分区域缓存，定期回写中心数据库，避免因实时跨地域读取数据导致游戏体验下降。

腾讯云在国内拥有北京、上海、广州三大数据中心，在海外还有北美、欧洲、亚太、南美等接入点供业务做分布部署和接入，如业务有使用缓存服务器则可直接选用腾讯云提供的 Redis 或 MongoDB 等存储产品，降低业务部署和运维门槛。

• 多地网络高速互联

多地同服最大的难点在于如何解决玩家跨服 PVP 等同服玩法网络延迟高问题，为了减少游戏接入服到全局中心服之间的时延，腾讯云可通过跨地域对等连接实现各大区私有网络之间高速数据同步，大大降低跨区间数据访问的网络时延。

操作步骤

1. 集中部署数据库，在靠近用户地域创建私有网络，详情请参见 [私有网络内部署数据库和云服务器](#)。
2. 利用 DNSPod 云解析智能调度功能实现玩家的就近访问，详情请参见 [DNSPod 云解析操作指南](#)。
3. 利用腾讯云跨地域对等连接实现不同地域的私有网络高速互联，详情请参见 [对等连接操作指南](#)。

VPN接入的混合云部署

最近更新时间：2018-06-09 16:15:46

根据您的连接需求，腾讯云分别提供两种服务连接您的企业数据中心和私有网络：VPN 连接和专线接入，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，是一种快速部署的高性价比选择。

- **专线接入**

提供一个您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。

下面将为您介绍如何使用 VPN 连接部署混合云。

应用场景

VPN 连接（VPN Connections）是一款通过 IPsec 加密通道连接您的企业数据中心和腾讯云私有网络（VPC）的服务，提供安全、可靠的加密通信。

目前 VPN 通道支持 IKE / IPsec 加密协议，最大支持 100M 带宽，如您有特殊需求，我们也可以为您提供定制化 VPN 接入服务，您可以提交 [工单申请](#) 与我们联系。

注意：

您需要为 VPN 通道占用的公网带宽付费，如果您的混合云互通带宽要求大于 200M，建议您选择 [专线接入的混合云](#) 部署方案。

VPN 通道的网络质量依赖于公网连接的网络质量，建议您在选择部署私有网络的地域时优先测试一下自有 IT 资源与腾讯云不同地域的网络时延，从而获得最优的混合云部署架构。

解决方案

- **云上数据中心**：在腾讯云创建的某个私有网络，部署云上数据中心。
- **连接方式**：VPN 连接。
- **网段规划**：物理数据中心与需要连接的私有网络之间**网段不可重叠**。

操作步骤

如何在腾讯云创建的某个私有网络部署云上数据中心，详情请参见 [操作指南](#)，本文不重复说明。

VPN 连接 可以在控制台实现全自助配置，您需要完成以下步骤 VPN 连接才能生效：

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。

详情请参见 [操作指南](#)。

专线接入的混合云部署

最近更新时间：2018-06-09 16:25:04

根据您的连接需求，腾讯云分别提供两种服务连接您的企业数据中心和私有网络：VPN 连接和专线接入，主要区别请参见 [VPN接入的混合云部署](#) 中的说明。

下面将为您介绍如何使用**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，有以下两种方式：

- **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：

腾讯云专线网关支持 NAT 功能，您私有网络和数据中心的**网段重叠不影响**双方通信。详情请参见 [专线接入](#) 说明。

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. 创建专线通道。
3. 创建专线网关接入专线通道，从而打通数据中心和您的 VPC。
4. （可选）配置专线 NAT。
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的备份。

详情请参见 [操作指南](#)。

基本概念

网关

最近更新时间：2018-06-09 16:33:25

公网网关

公网网关是开启了转发功能的云服务器，无外网 IP 但需进行 Internet 访问的云服务器可通过位于非相同子网公网网关转发来访问 Internet。

NAT网关

- NAT 网关和公网网关类似，是私有网络内云服务器访问公网的另外一种方式。NAT 网关底层实现采用双机热备，单机故障可在不影响网络连接的情况下切换至备用设备，保障网络出口高可用。
- NAT 网关提供了三种配置类型，最大满足 5Gbps 突增流量和 1000W 并发连接数。
- NAT 网关设备共收取两项服务费用：网关租用费（按小时计费）和访问 Internet 产生的流量费用，详情请参见[价格总览](#)。
- NAT 网关与公网网关都用于私有网络内云服务器访问 Internet，但二者也存在一些差异，如下表所示：

属性	NAT网关	公网网关
可用性	双机热备，自动热切换	手动切换故障网关
公网带宽	最大 5Gbps	取决于云服务器网络带宽
公网IP	最多绑定 10 个弹性 IP	1 个弹性 IP or 普通公网 IP
公网限速	无	取决于云服务器限速
最大连接数	1000W	50W
内网 IP	不占用私有网络用户的内网 IP	占用子网内 IP
安全组	NAT 网关不支持绑定安全组，可以对 NAT 网关后端云服务器绑定安全组	支持
网络 ACL	NAT 网关不支持绑定网络 ACL，可以对 NAT 网关后端云服务器所在子网绑定网络 ACL	公网网关不支持绑定网络 ACL，可以对公网网关所在子网绑定网络 ACL

属性	NAT网关	公网网关
费用	大陆地区： 小型（最大 100W 连接数）：0.5 元 / 小时 中型（最大 300W 连接数）：1.5 元 / 小时 大型（最大 1000W 连接数）：5 元 / 小时	取决于作为公网网关的云服务器规格，以大陆地区为例： 1 核 2G：0.44 元 / 小时 4 核 8G：1.76 元 / 小时 12 核 24 G：5.28 元 / 小时

VPN 网关

VPN 网关是私有网络与用户 IDC 之间建立的加密网络通道的一端（另一端为对端网关），主要用于建立安全可靠的混合云连接。

对端网关

对端网关指用户的私有云机房，用户只需要提供机房的自定义名称及公网 IP 即可建立一个对端网关。私有网络的 VPN 网关可与多个对端网关建立带有加密的 VPN 网络通道。

VPC 内可部署的其它服务

最近更新时间：2018-06-09 16:40:36

腾讯云私有网络（VPC）是由许多其他腾讯云服务集成，它们之间的关系如下表所示：

计算与网络服务

产品	与 VPC 的关系
云服务器 CVM	可将云服务器部署在 VPC 中
负载均衡 CLB	可在 VPC 内部署内网 LB 或者公网 LB
NAT 网关	可用于 VPC 内流量访问 Internet
对等连接 PC	可用于连接多个地域的 VPC
VPN 连接	通过 IPsec VPN 连接 VPC 和用户 IDC
专线接入 DC	通过专线连接 VPC 和用户 IDC
基础监控 BCM	为 VPC 内某些服务的关键指标提供自定义告警

数据库服务

产品	与 VPC 的关系
云数据库 MySQL	可在 VPC 部署该数据库服务，该服务将占用 VPC IP 资源
云数据库 SQLServer	可在 VPC 部署该数据库服务，该服务将占用 VPC IP 资源
云数据库 TDSQL	可在 VPC 部署该数据库服务，该服务将占用 VPC IP 资源
云数据库 PostgreSQL	可在 VPC 部署该数据库服务，该服务将占用 VPC IP 资源
云缓存 Memcached	可在 VPC 部署该数据库服务，该服务将占用 VPC IP 资源

产品	与 VPC 的关系
云数据库 MongoDB	可在 VPC 部署该数据库服务，该服务将占用 VPC IP 资源
云数据库 HBase	可在 VPC 部署该数据库服务，该服务将占用 VPC IP 资源