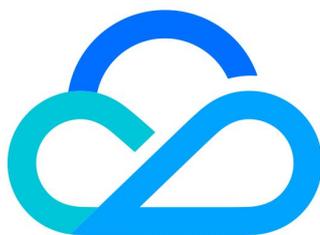


负载均衡

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

负载均衡简介

产品优势

使用场景

技术原理

服务等级协议

使用约束

产品简介

负载均衡简介

最近更新时间：2018-10-08 10:29:30

什么是负载均衡？

负载均衡（Cloud Load Balancer）是对多台 [云服务器](#) 进行流量分发的服务。负载均衡可以通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提升应用系统的可用性。

负载均衡服务通过设置虚拟服务地址（VIP），将位于 **同一地域** 的多台云服务器资源虚拟成一个高性能、高可用的应用服务池；根据应用指定的方式，将来自客户端的网络请求分发到云服务器池中。

负载均衡服务会检查云服务器池中云服务器实例的健康状态，自动隔离异常状态的实例，从而解决了云服务器的单点问题，同时提高了应用的整体服务能力。

腾讯云提供的负载均衡服务具备自助管理、自故障修复，防网络攻击等高级功能，适用于企业、社区、电子商务、游戏等多种用户场景。

组成部分

一个提供服务的负载均衡组通常由以下部分组成：

- CloudLoadBalancer：负载均衡实例，用于流量分发。
- VIP(virtual IP)：负载均衡向客户端提供服务的 IP 地址。
- Backend/Real Server：后端一组云服务器实例，用于实际处理请求。
- VPC/基础网络：整体网络环境。

来自负载均衡外的访问请求，通过负载均衡实例并根据相关的策略和转发规则分发到后端云服务器进行处理。

名词解释

术语	全称	说明
负载均衡器	Cloud Load Balancer	腾讯云提供了一种网络负载均衡服务，可以结合 CVM 云服务器为用户提供基于 TCP/UDP 以及 HTTP 负载均衡服务

术语	全称	说明
负载均衡监听器	Load Balance Listener	负载均衡服务监听器，包括监听端口、负载均衡策略和健康检查配置等，每个监听项对应后端的一个应用服务
后端服务器	Real Server	接受负载均衡分发请求的一组云服务器实例，负载均衡服务将访问请求按照用户设定的规则转发到这一组后端 CVM 上进行处理
虚拟服务地址	Virtual IP	系统分配的服务地址，当前为 IP 地址。用户可以选择该服务地址是否对外公开，来分别创建公网和私网类型的负载均衡服务

负载均衡的工作原理

基本工作原理

负载均衡器接受来自客户端的传入流量，并将请求路由到一个或多个可用区的后端云服务器实例上进行处理。

负载均衡服务主要由负载均衡监听器提供。监听器负责监听负载均衡实例上的请求、执行策略分发至后端服务器等服务，通过配置 客户端-负载均衡 和 负载均衡-后端服务器 两个维度的转发协议及协议端口，负载均衡可以将请求直接转发到后端云服务器上。

建议您跨多个可用区配置负载均衡器的后端 CVM 实例。如果一个可用区变得不可用，负载均衡器会将流量路由到其他可用区正常运行的实例上去，从而屏蔽可用区故障引起的服务中断问题。

请求路由选择

客户端请求通过域名访问服务，在请求发送到负载均衡器之前，DNS 服务器将会解析负载均衡域名，并将收到请求的负载均衡 IP 地址返回到客户端。当负载均衡监听器收到请求时，将会使用不同的负载均衡算法将请求分发到后端服务器中。目前腾讯云支持加权轮询和 ip_hash 加权最小连接数等多种均衡算法。

监控后端服务状态

负载均衡器还可以监控后端实例的运行状况，从而确保只将流量路由到正常运行的实例上去。当负载均衡器检测到运行不正常的实例时，它会停止向该实例路由流量，然后会在它再次检测到实例正常运行之后重新向其路由流量。

相关服务

负载均衡可与以下服务一起使用来提高应用程序的可用性和可扩展性：

- CVM 实例：应用程序在云上运行的虚拟服务器。有关更多信息，请参见 [CVM 产品文档](#)。
- 弹性伸缩：弹性地控制实例数量。在弹性伸缩中启用负载均衡实例，则伸缩的实例将自动加入负载均衡组，同时终止的实例将自动从被移出负载均衡组。有关更多信息，请参见 [弹性伸缩 产品文档](#)。

-
- 云监控：帮助您监控负载均衡及所有后端实例的运行状况并执行所需操作。有关更多信息，请参见 [云监控 产品文档](#)。
 - 域名注册和域名解析：通过将您自定义的域名（例如 `www.example.com`）转换为网络通信所用的 IP 地址（例如 `192.0.2.1`），快速便捷地将请求路由至负载均衡实例。有关更多信息，请参见 [域名注册 产品文档](#) 和 [域名解析 产品文档](#)。

产品优势

最近更新时间：2018-06-01 17:06:34

负载均衡服务是否优秀，主要是由以下纬度的性能测试指标来评判的：

- TPS（每秒新建连接数）：负载均衡实例每秒新建 TCP 连接的能力。
- 最大并发连接数：并发连接数指的是客户端向服务器发起请求并建立了 TCP 连接的总数。亦即每秒钟服务器链接的总 TCP 数量。
- QPS(query per second)：也可以叫 RPS，每秒请求。请求数指的是客户端在建立完连接后，向 HTTP 服务发出 GET/POST/HEAD 数据包。
- 吞吐量：负载均衡实例可支持的总的流量带宽。

腾讯云提供高性能的负载均衡服务：

- 负载均衡单集群提供超过 1.2 亿 的最大连接数，轻松应对亿级 Web 业务访问量。
- 负载均衡单集群可处理峰值 40Gb/s 的流量，每秒处理包量（PPS）可达 600 万。
- 对每个租户的流量进行严格隔离，提供主动 DDoS 防护能力。当遭遇 DDoS 攻击时，腾讯云负载均衡能为您免费提供 2~10 Gb DDoS 攻击峰值流量的防御能力。

注意：

如果您对峰值流量有更高的要求，则需要另行购买，选购 [BGP高防产品](#)，最高可为您提供 300 Gb 攻击峰值流量的防御能力。

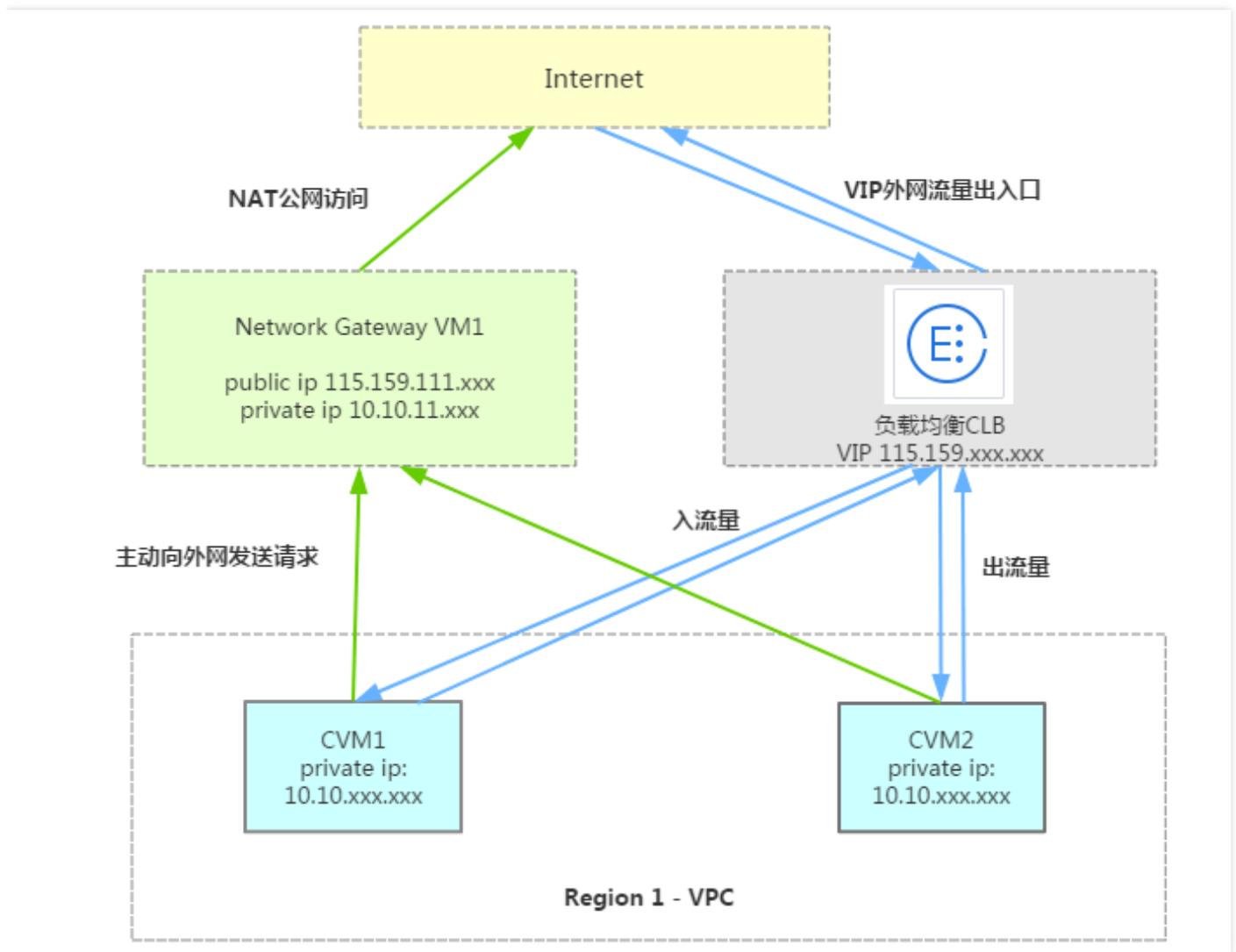
使用场景

最近更新时间：2018-07-16 10:56:17

负载均衡主要可以应用于以下场景中：

- 横向扩展应用系统的服务能力，适用于各种web server和app server。
- 消除应用系统的单点故障，当其中一部分CVM实例宕机后，应用系统仍能正常工作。

以下是一个四层协议中双向隐藏（出访公网/公网访问）后端服务器集群的例子：



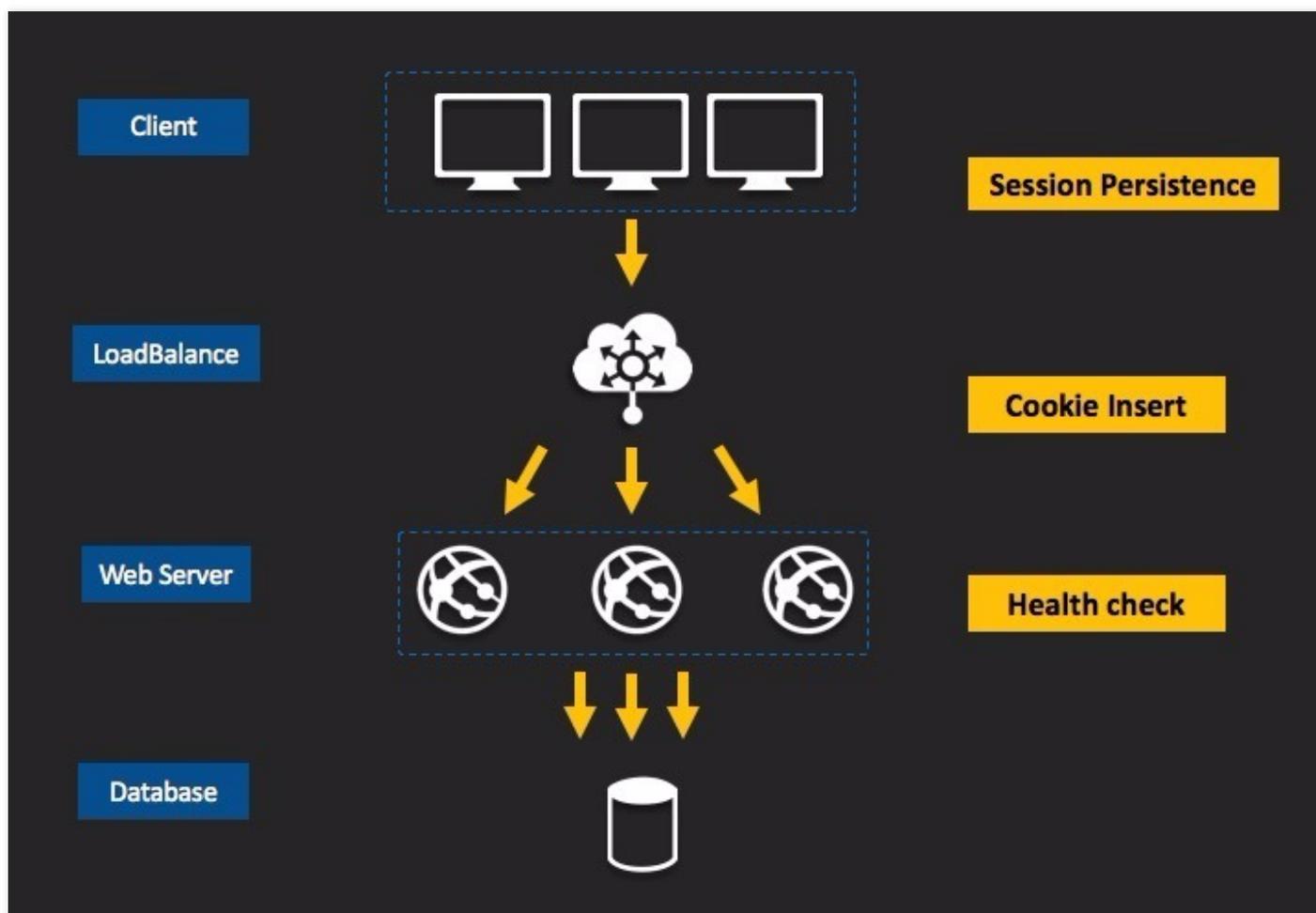
云服务器（CVM1、CVM2）部署在region1的VPC中，不具备公网IP，不可主动与公网通信。

- 当Internet上的资源访问云服务器上的服务时，必须通过统一的负载均衡服务VIP（115.159.xxx.xxx）进行访问。负载均衡器负责将所有请求使用一定的均衡策略分发到后端的服务器上，Internet对后端服务器集群完全无感知。后端服务器处理请求后，回包流量也通过负载均衡返回客户端，做到了对后端服务器的有效隐藏。

- 当云服务器集群需要主动出访公网时，不经过负载均衡，通过配置路由表并通过一个Internet网关（VM1）进行NAT转发。对于Internet上的资源来说，请求的地址始终为Internet网关的公网IP（115.159.111.xxx），Internet上的资源对后端服务器集群完全无感知，做到了服务器端的隐藏，提升了后端服务器的安全性。

流量分发

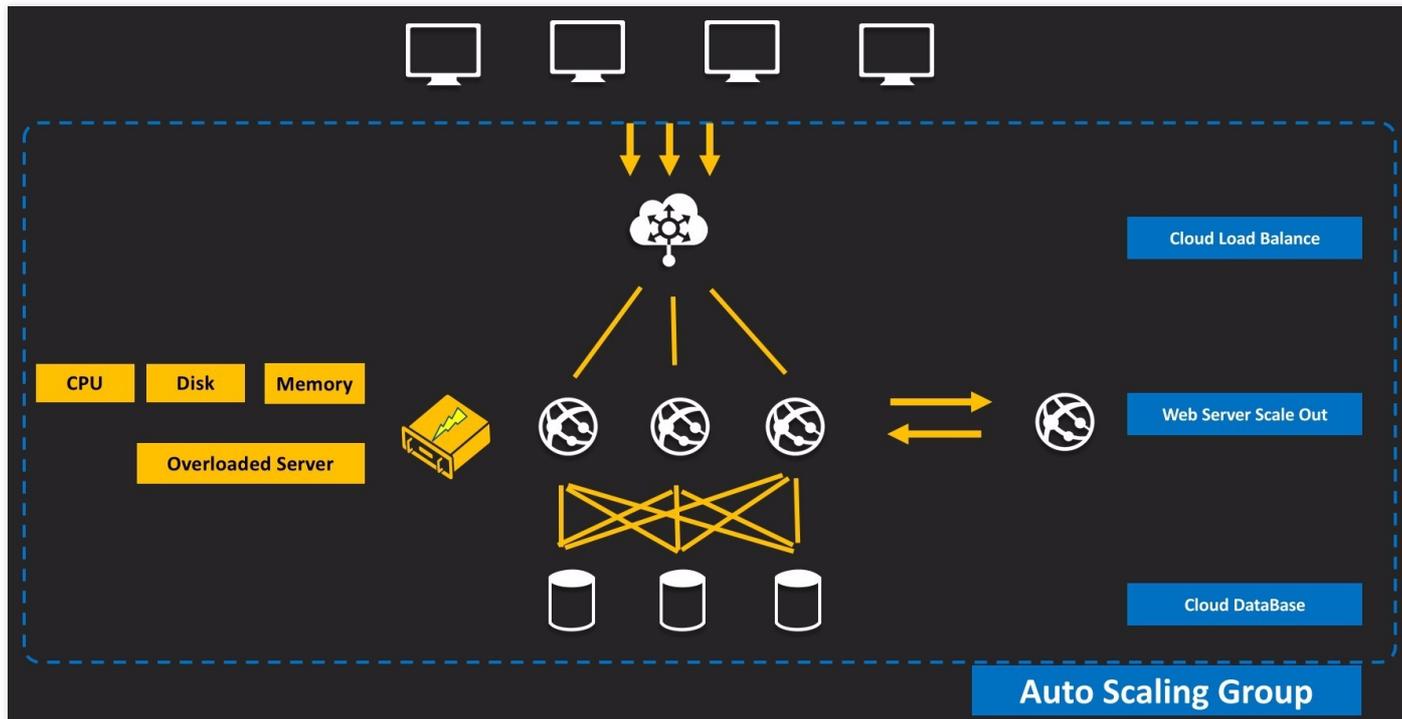
- 通过设置负载均衡的虚拟服务地址（VIP）和网站域名，将多台web接入层服务器虚拟成一个高性能、高可用的接入层服务池，所有的公网请求都通过CLB进入，既安全又节省了公网ip地址。
- 负载均衡将保证请求会均匀的转发到每一个接入层服务器，接入层服务器可使用廉价的、配置一致的云服务器，或Docker容器来承载



横向扩展

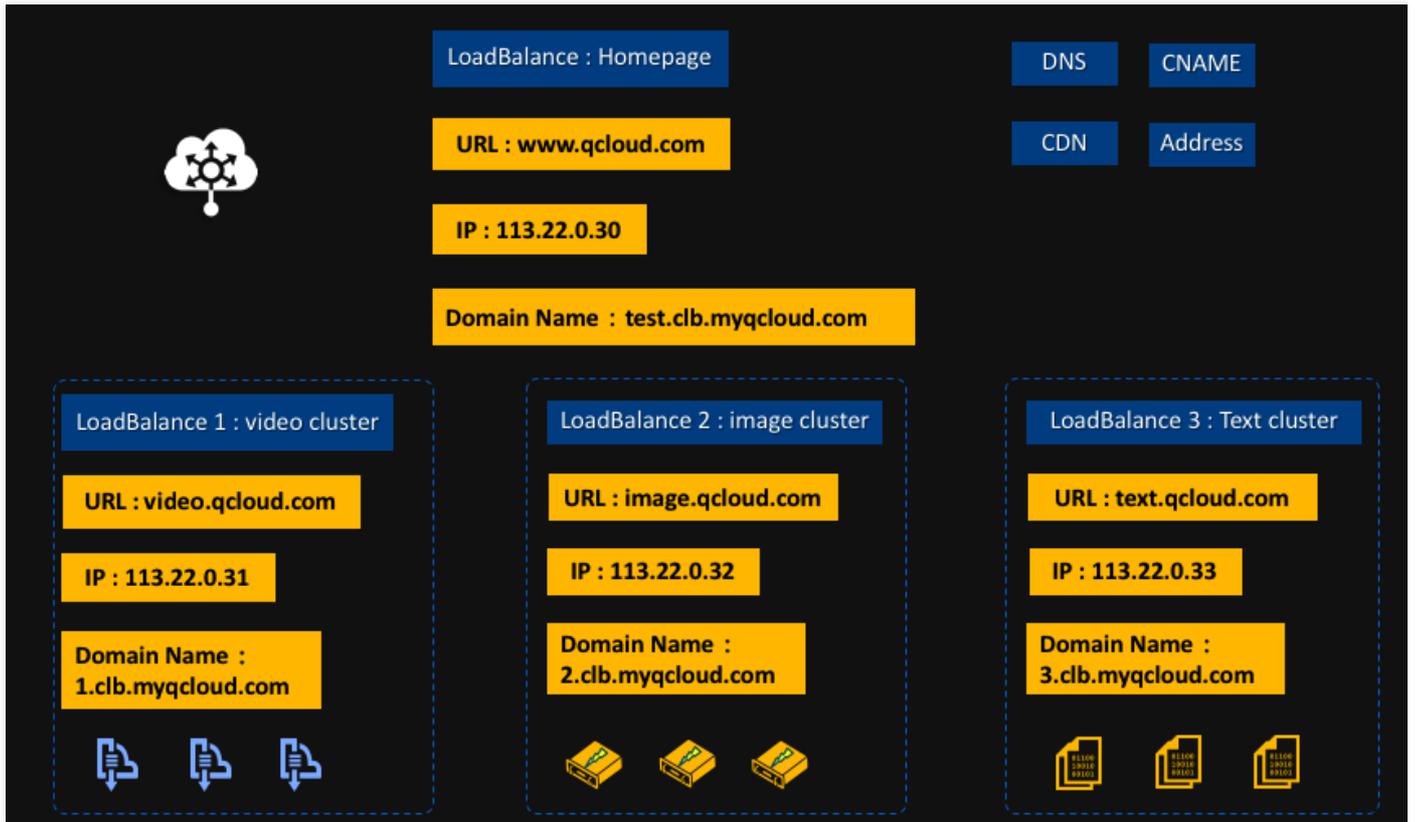
- 负载均衡结合Autoscaling动态伸缩组，可为您自动创建和释放CVM实例。接入层web服务器可随公网的访问压力的增加/减少，响应的增加/减少。

- 电商行业的的双11、6.18等大促销活动，web访问量可能瞬间陡增10倍，且只持续短暂的数小时。使用负载均衡及Autoscaling能最大限度的节省IT成本



业务分离

- 典型的WEB业务如论坛、网站等，建议将图片服务、文本服务等不同业务进行分离，便于网页开发迭代
- 业务分离后，每个负载均衡实例及后端关联服务器组作为一个独立的业务集群
- 在DNS服务商（如DNSpod）可添加多条A记录，从而实现不同业务之间的域名跳转、重定向
- 大型网站常有上百个业务子模块，使用负载均衡及DNS解析，对外的门户网站首页的访问地址，可收敛为负载均衡的1个公网地址以及1个自有域名。便于client端客户的访问



技术原理

最近更新时间：2018-05-31 11:23:35

<p>视频教程</p> <p>四层负载均衡原理及应用</p> <p>▶ 视频 04'14"</p>	<p>视频教程</p> <p>七层负载均衡原理及应用</p> <p>▶ 视频 02'32"</p>	<p>视频教程</p> <p>负载均衡的轮询方式和高可靠性</p> <p>▶ 视频 07'19"</p>
---------------------------------------------------	---------------------------------------------------	------------------------------------------------------

底层实现

腾讯云负载均衡CLB当前提供四层和七层上的负载均衡服务，由腾讯发起的Tencent gateway (TGW) 统一网关产品提供负载均衡能力，具有可靠性高、扩展性强、性能高、抗攻击能力强等特点，可支持大规模的并发访问，并防止恶意攻击的流量。CLB的产品形态包括：提供负载均衡能力，收敛外网IP，抗DDoS攻击，QoS，支持FTP、SIP等能力。

负载均衡采用集群部署，可实现会话同步，以消除服务器单点，提升冗余，保证服务稳定。已在同一个地域部署多个机房，实现同城容灾。

本章主要介绍CLB的几个关键技术点，从平台纬度、资源纬度到业务纬度分析CLB通过哪些技术来实现云平台的租户隔离、架构容灾、资源容灾、抗攻击等能力。

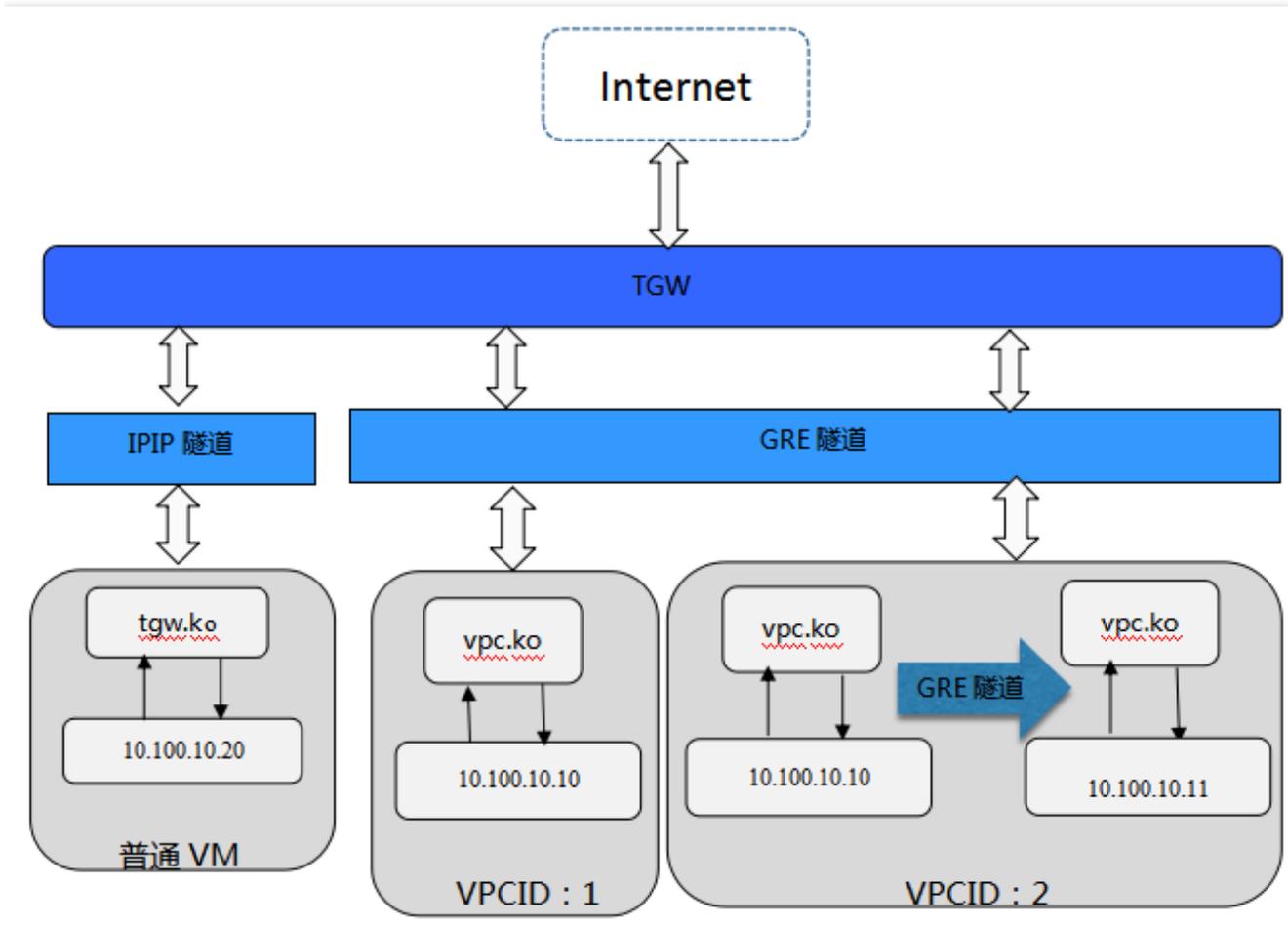
注：本文RS指绑定CLB负载均衡器的CVM云服务器。VIP指CLB负载均衡器对外服务的IP地址。

租户隔离

云平台一个关键的能力就是租户隔离，接入云的用户都希望自己的业务不受别人的影响，至少在网络上能够隔离，别人不能随意访问我的机器。当然这个功能业界有多种实现方式，比较常用的是在硬件上做隔离，使用特定的接入交换机，采用vxlan协议来达到隔离的目的。这么做的缺点是：

1. 需要使用特殊的交换机；
2. 需要额外的设备打通vxlan网络和普通网络，这样就存在单点问题；
3. 不易于与现有的网络环境兼容。

基于以上原因，我们采用了软件的方案，通过IP隧道+VPC的方式来实现租户隔离。



从图中左侧我们可以看到，CLB和Rs之间的交互采用的IP隧道方式，云服务器CVM（RS）分配实际的内网IP，和物理网络是打通的。这样做的好处是实现简单，能够兼容以前的物理机方案，但是缺点在于：

1. 需要额外的模块实现租户间隔离；
2. 租户之间内网IP无法重用，无法实现自由组网；
3. 由于IP在内网唯一，迁移时必须变换Rs IP，因此也无法实现热迁移。

基于以上原因，腾讯云开发出VPC私有网络。在上图右侧可以看到同一个租户分配一个VPCID，在VPC内，客户可以自由组网，租户网络本身就是隔离的，具体的处理由vpc.ko内核模块来实现。

IP收敛

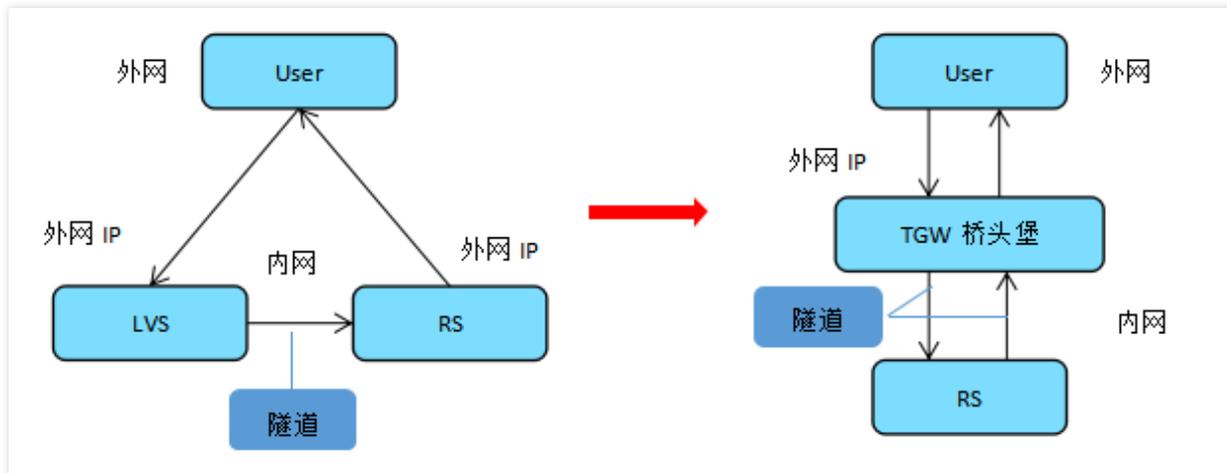
提起负载均衡，业界最著名的非LVS（Linux Virtual Server）技术莫属。

LVS共有三种模式：DR模式、NAT模式及TUNNEL模式。其中DR模式主要的限制是要求LVS和RS必须在同一个vlan，部署起来限制很大，并且可扩展性较差；NAT模式主要的缺陷在于RS的回包需要使用默认路由，同样存在扩展性的问题；因此我们最初搭建LVS集群采用的是TUNNEL模式。然而TUNNEL模式要求每台RS都需要分配外网IP。对于腾讯云以及RS较多的业务，外网IP是一个很大的挑战。

基于以上原因，CLB应运而生。

下图是之前使用的LVS方案和CLB方案的一个简图，主要区别在于：

1. CLB不需要给RS分配外网IP，起到收敛IP的作用；
2. 出流量仍然通过CLB，更易于定位问题，另外对于业务流量形成闭环，起到桥头堡的作用。



高可靠实现

高可靠是衡量云服务的一个重要指标。CLB 为了实现高可靠的服务，我们进行了以下的方案实现：

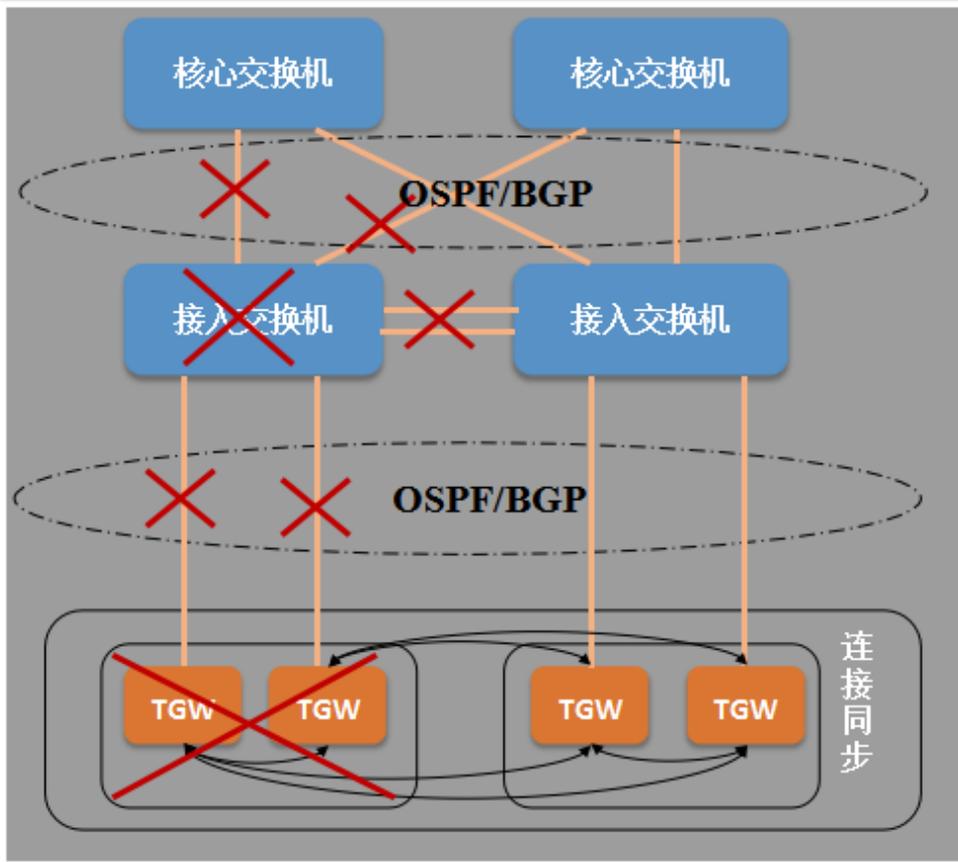
1. 集群容灾；
2. session同步；
3. 资源隔离；
4. 抗DDos攻击。

集群容灾和session同步

集群容灾，简单来说就是一个集群中一台服务器倒掉不会影响整个集群的服务能力。传统的集群容灾采用的HA模式（vrrp协议），常见的开源方案如LVS，传统方式的缺点在于：一个集群同时只有一半的服务器在工作，另外一半的机器处于冷备状态；死机之后的切换速度相对较慢。

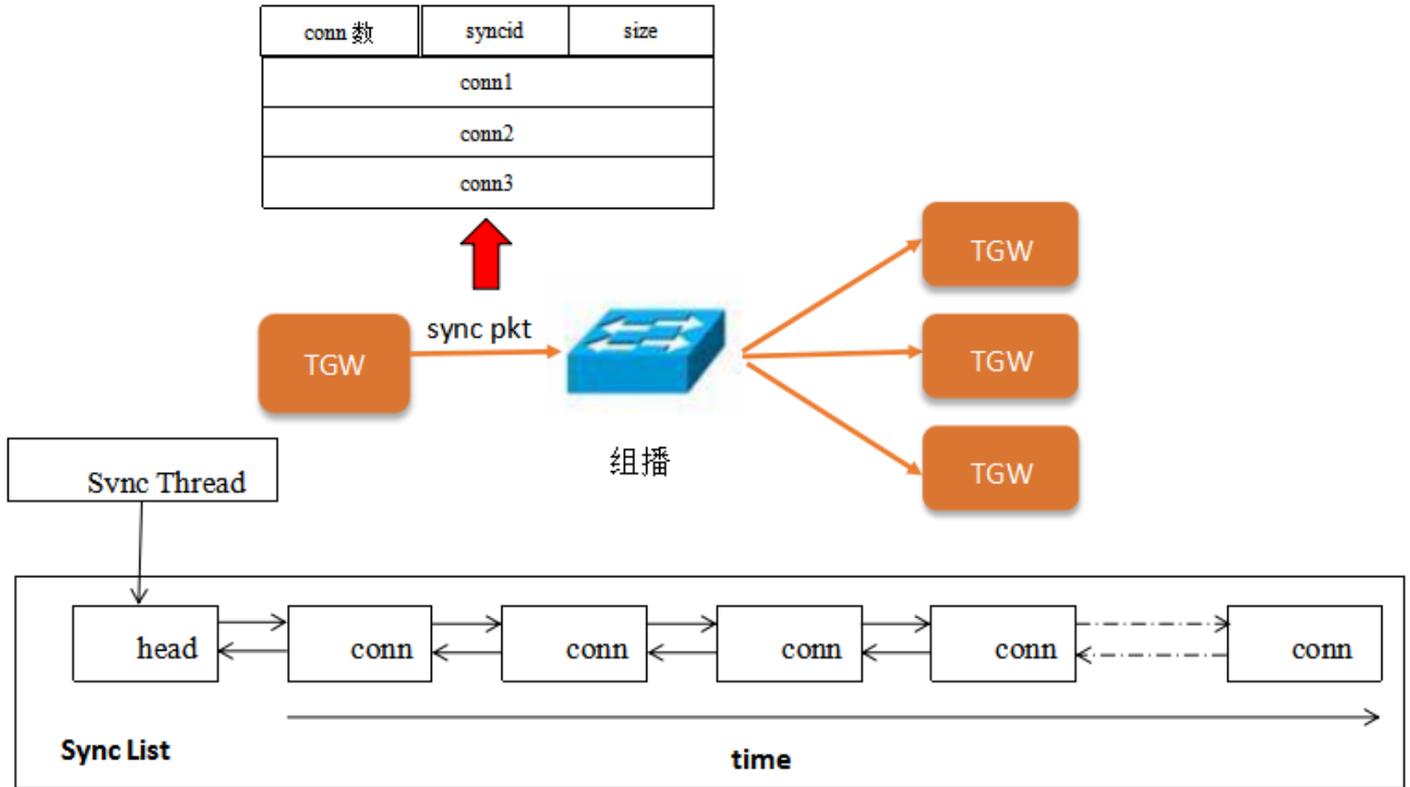
CLB在设计之初就考虑到这个问题，采用ospf动态路由协议来实现集群的容灾，若一台机器倒掉，ospf协议可以保证在10s以内把机器从集群中剔除。CLB一个集群放在两个接入交换机下，并且保证跨机架的容灾，这样保证在即便有单边的交换机出故障或者单边机架掉电时，本集群的服务不受影响。

集群容灾保证CLB集群的可用性，但是对于一个客户来讲，如果服务器倒掉，即便该机器被剔除了，也只能保证新的连接不会落在这台机器，那么长连接就会断掉。为了解决这个问题，我们实现了集群内session连接定期同步。这样在别的服务器接管故障机器的包时，能够正确找到session，保证提供正常服务。



LVS的做法：连接状态变化时同步；在长短连接并存的情况下，短连接业务的同步流量非常大，会对正常转发造成冲击。

CLB解决方案：每个连接创建5秒后才同步，连接如果在5秒内，则不同步；只同步‘长连接’。

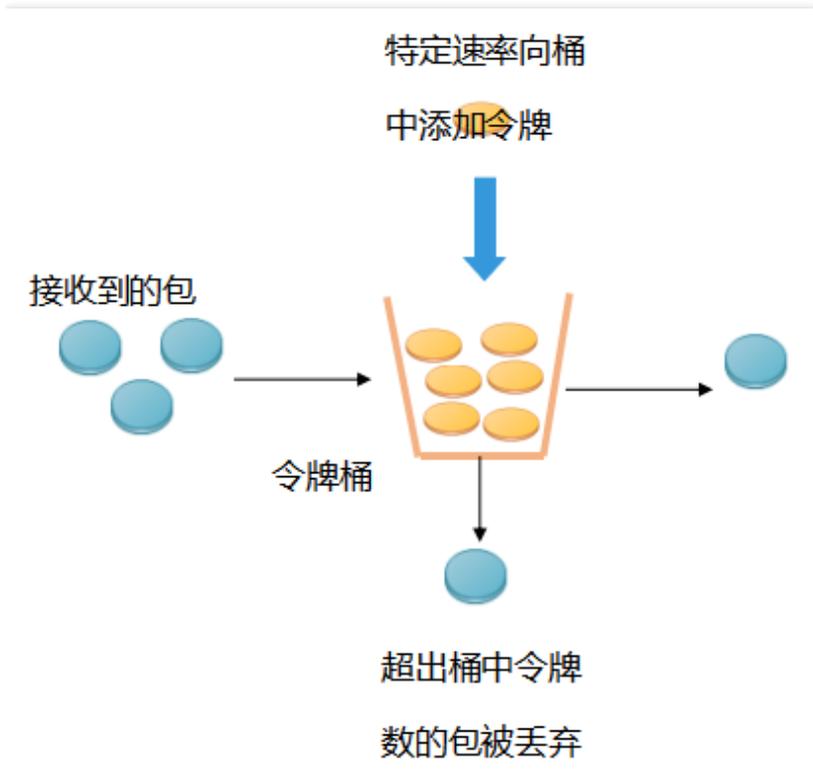


资源隔离

资源隔离功能，是为了在个别业务受到攻击时，CLB出现高负载的情况下，保护别的业务不会受到影响。

具体实现是：定期（5s）检测CLB是否达到配置的高负载的警戒线，如果达到了则开启资源隔离，CLB将检测每个业务的流量、包量、连接数，超过上限的就丢弃，保证CLB服务器不会达到真正的高负载而影响别的业务。在正常情况下，资源隔离功能是关闭的；只有当业务突增放量，或者某个业务被攻击导致CLB达到警戒线时，保证在5s以内开启该功能，保证正常的业务转发不受影响。

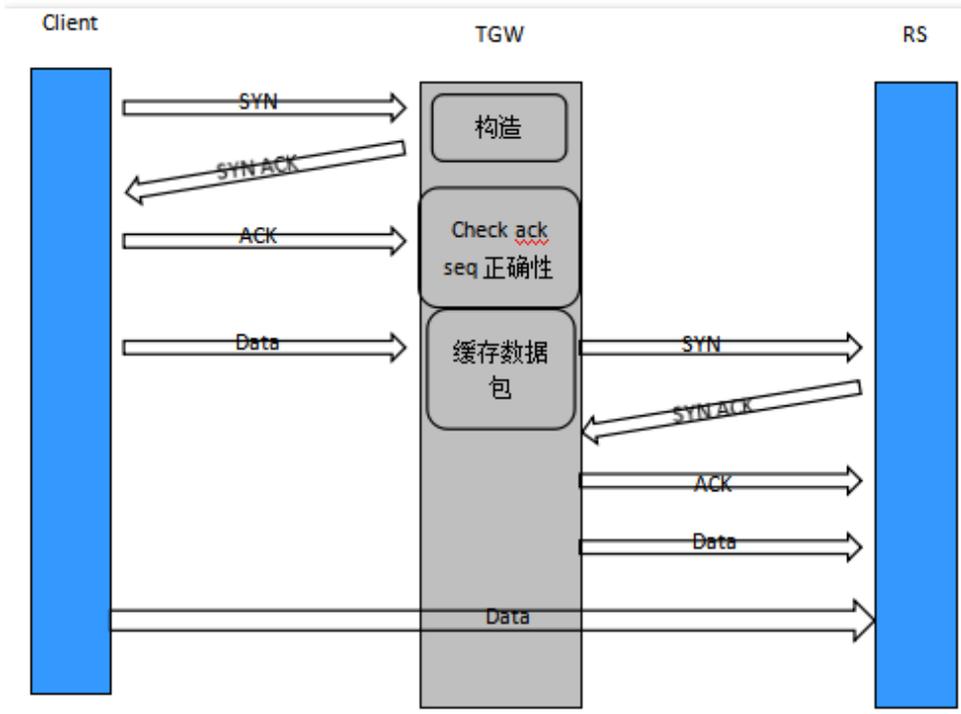
资源隔离采用经典的令牌桶算法，工作过程是：定期向桶中放置一定量的令牌，每到一个包，消耗一个令牌，在一段时间内令牌耗尽，则开始丢包。



抗DDoS攻击

集群容灾和资源隔离都是为了保护CLB平台自身，而对于单个业务，如果被攻击，则受伤害的概率就是100%，CLB是不允许这种情况发生的。当然对于DDoS攻击，腾讯云有非常强大的大禹系统来保护业务，但是大禹系统的宙斯盾的检测时长是10s，那么在大禹系统生效之前，可能客户的RS已经被压垮。为了解决这10s内的问题，我们开发了synproxy的功能。

具体实现是：CLB在接收到客户端的三步握手请求时，代理三步握手，在数据包到来之前，不会打扰到RS，一旦第一个包到来，CLB将其缓存，此时再和RS进行三步握手，握手成功之后，将缓存的数据包发送给RS，之后的流程就透传数据包了。这样保证DDoS攻击不会到达RS，而是由CLB来承担压力。CLB本身承载能力比较强，又是集群模式，同时又具备资源隔离的能力，所以一般情况下，很难在10s以内把CLB机器压垮。



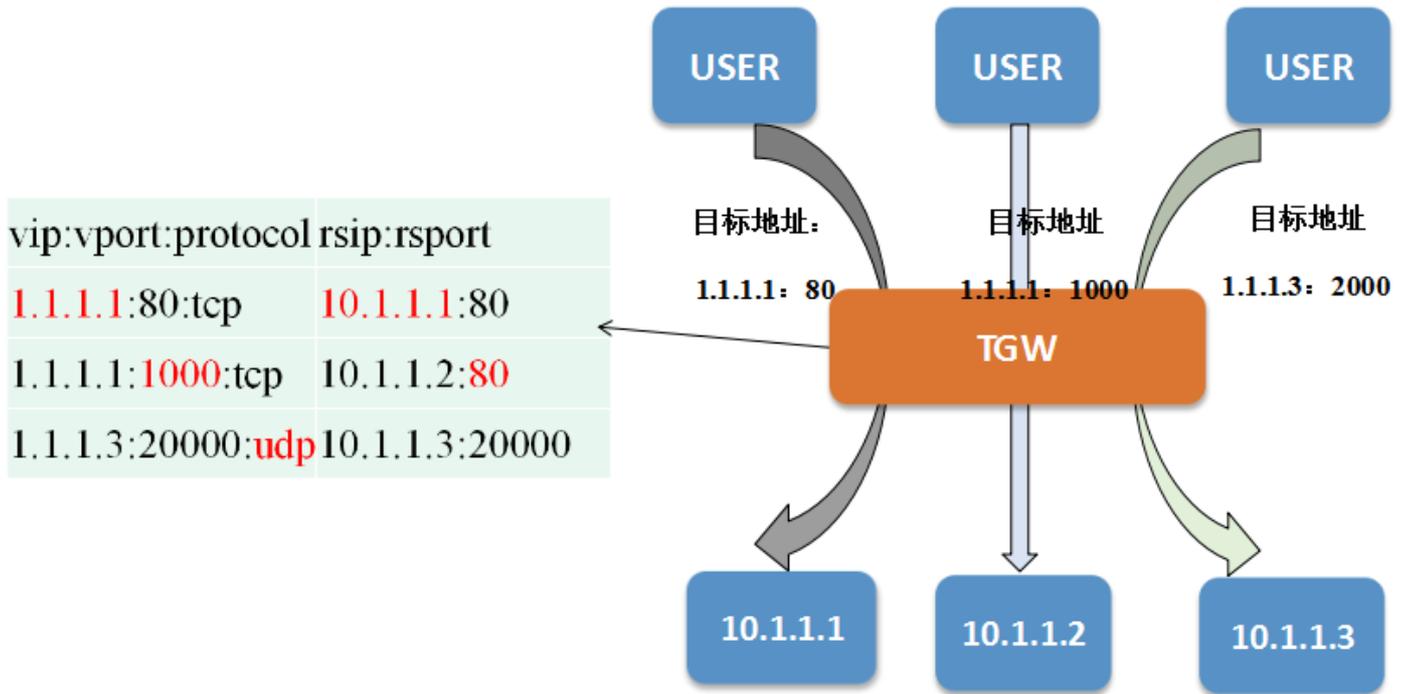
腾讯云负载均衡不同类型的特点

腾讯云CLB负载均衡器目前提供了四层和七层协议的转发能力：

- 4层负载均衡，对应监听器的tcp和udp；
- 7层负载均衡，对应监听器的http/https能力。

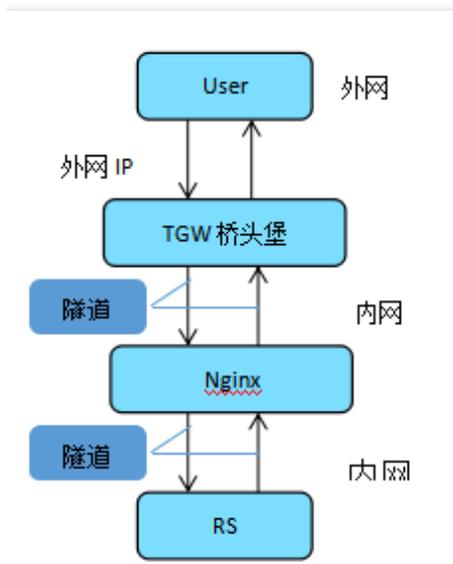
4层负载均衡

4层负载均衡是CLB最早实现的方案，也是作为一款负载均衡产品必备的功能。基本原理就是在CLB上通过端口来区分不同的业务，转发规则（rule）的key：vip:vport:protocol，目前QCloud中使用最多的就是这种负载均衡方式，但是在QCloud中，VIP是属于同一个开发商的，不同开发商之间的流量严格隔离。



7层负载均衡

无日租型的方案能够应对普通的7层负载均衡服务，但是对于有session和cookie需求的7层用户，就得自己搭建自己的nginx来在做一层反向代理，不但浪费，可靠性也会受到影响。

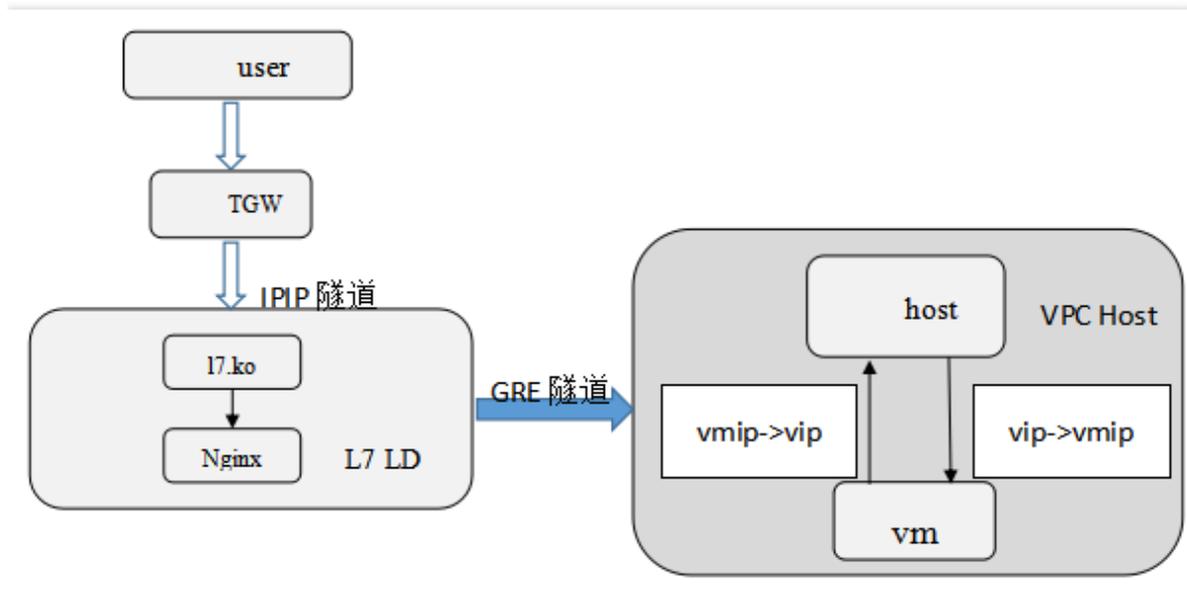


7层负载均衡在设计之初讨论了2种方案：

1. 外网IP直接起在nginx机器上，搭建nginx集群
2. nginx集群接在4层CLB之下

方案1存在的弱点是对DDos攻击束手无策，对于腾讯云来说，需要一个VIP可同时接入4层和7层，而方案1无法做到，因此最终我们采取了方案2。此外方案2还有一个优势是可以很方便的动态扩缩容，这样利于应对业务要求快速扩容的场景。

但是，nginx本身是通过反向代理来实现负载均衡功能的，在腾讯云上存在一个致命的问题：由于vpc网络是虚拟网络，和物理网络之间是通过母机来打通的，7层LD和RS之间没办法直接使用nginx的反向代理功能。因此，我们想到了模拟4层，在7层LD上插入了l7.ko内核模块，用于负责封装gre隧道和IP隧道和RS之间交互。



服务等级协议

最近更新时间：2017-05-10 15:27:16

业务可用性

负载均衡承诺99.95%的业务可用性，即用户每月负载均衡可用时间应为30天×24小时×60分钟×99.95%=43178.4分钟，即存在43200-43178.4=21.6分钟的不可用时间，同时适用于4/7层负载均衡vip。

云服务器出现故障时，负载均衡将自动剔除此故障云服务器，并由其他云服务器接管故障服务器的流量，此类故障不属于负载均衡故障统计时间范畴内。

业务故障的恢复正常时间5分钟及以下的，不计入业务不可用性计算中，不可用时间指业务发生故障开始到恢复正常使用的时间，包括维护时间。

网络接入能力

用户购买的负载均衡具备自适应的网络接入能力，根据用户关联云服务器带宽自动增减网络接入能力，公网出口带宽由关联主机公网带宽决定。腾讯云负载均衡出口采用BGP多线接入，保障用户网络接入质量。

业务资源调配能力

腾讯云负载均衡以集群方式实现，具备弹性扩缩容能力，可根据用户的服务规模自动扩容。用户只需要根据业务规模增加或减少关联在负载均衡上的云服务器数量及带宽即可自助实现弹性能力调度。

数据可审查性

腾讯云在依据现有法律法规体系下，出于配合政府监管部门的监管或安全取证调查等原因的需要，在符合流程和手续完备的情况下，可以提供负载均衡相关信息，包括关键组件的运行日志、运维人员的操作记录、用户操作记录等信息。

故障恢复能力

腾讯云提供专业团队7×24小时全面维护，并以工单和电话保障等方式提供技术支持，具备完善的故障监控、告警、定位及故障恢复能力。

使用约束

最近更新时间：2018-09-25 14:43:01

腾讯云负载均衡使用时有一些通用限制，不同类型的负载均衡实例也有该类型特定的使用限制。有关负载均衡类型的更多内容，请参考 [公网负载均衡](#) 和 [内网负载均衡](#)。

	特定限制	通用限制
应用型负载均衡实例	在同一个负载均衡实例中，一个前端端口只能对应一种协议 在同一个负载均衡实例中，一个前端端口可以对应多个后端端口 一个监听器下允许创建 50 个转发规则 一个转发规则内允许添加 100 个转发组（deviceid + port，即云服务器 + 端口）	每种类型的 CLB 累计可购买 100 台 每台 CLB 实例最多关联 100 台服务器 每台 CLB 实例最多创建 50 个监听器
传统型负载均衡实例	在同一个负载均衡实例中，一个前端端口只能对应一种协议 在同一个负载均衡实例中，一个前端端口对应一个后端端口	端口数仅能为 1 - 65535 的整数

若 CLB 关联的云服务器 CVM 由于欠费被隔离（如进入回收站，或按量计费被清退的云服务器），CLB 会强制解除与该云服务器的绑定关系。