

硕 士 研 究 生 读 书 报 告



题目 虚拟私有网络在云计算上的组织扩展

作者姓名 汤建华

作者学号 21651084

指导教师 李启雷

学科专业 移动互联网与游戏开发

所在学院 软件学院

提交日期 二○一七年一月

Organizational expansion of virtual private networks in cloud computing

A Dissertation Submitted to

Zhejiang University

in partial fulfillment of the requirements for

the degree of

Master of Engineering

Major Subject: Software Engineering

Advisor: Li Qilei

By

Tang Jianhua

Zhejiang University ,P.R. China

2017

摘要

随着互联网的快速发展，大数据，云计算行业也快速成型。云计算在国内外产业界学术界发展速度惊人。云计算服务主要包括计算域，存储域，网络域三大块，本文将对网络域的虚拟私有网络（VPC）组成架构进行分析。了解网络组是如何实现网络的安全组，防火墙，对等连接，弹性IP，VPN，弹性负载均衡等，保障网络数据中心的安全可靠。

**关键词**：虚拟私有云，弹性IP，VPN专线，对等连接，弹性负载均衡，安全组，防火墙

Abstract

With the rapid development of the Internet, large data, and the cloud computing industry is also rapidly forming. The development of cloud computing in the academic circles of industrial circles at home and abroad is astonishing. The cloud computing service mainly includes computing domain, storage domain and network domain three blocks. This paper will analyze the virtual private network (VPC) structure of network domain. Understand how network group implements network security group, firewall, peer-to-peer connection, resilient IP, VPN, elastic load balancing, and so on, so as to ensure the safety and reliability of network data center.

**Keywords：**Virtual private cloud, elastic IP, VPN, elastic load balancing, security group, firewall

1云计算的概念和关键技术

云计算是网格计算、分布式计算、并行计算、效用计算、网络存储、虚拟化、负载均衡等传统计算机技术和网络技术发展融合的产物。云计算将计算从用户终端集中到“云端”，是基于互联网的计算模式。按照云计算的运营模式，用户只需关心应用的功能，而不必关注应用的实现方式，即各取所需，按需定制自己的应用。最简单的云计算技术在网络服务中已经随处可见，例如搜索引擎、网络信箱等，使用者只要输入简单指令即能得到大量信息。云计算不仅仅用于资料搜寻和分析，未来还可用于分析DNA结构、基因图谱定序等。“云计算”的模式具有规模经济性，所有应用通过互联网提供给多个外部用户，多个用户共享同一个应用，进而实现计算在用户间的共享，提高处理器和存储设备的利用率。

云计算的主要模式包括软件即服务SAAS，平台服务PAAS，基础服务IAAS层。大体可以任务依次服务内容减少，从上层软件，到平台，到基础设备。

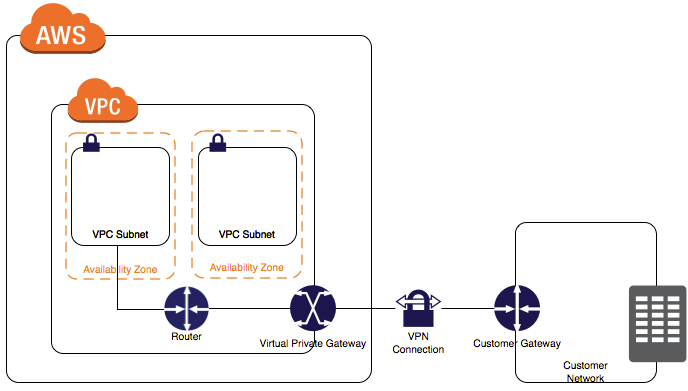
重点发展企业有国外有亚马逊，思科，IBM，甲骨文，惠普等国内有阿里，百度，腾讯，华为，联想，中国移动等在扩展云业务。

**2虚拟私有网络**

虚拟私有云（VPC）是一个公共云计算资源的动态配置池，需要使用加密协议、隧道协议和其他安全程序，类似于VPN。

VPC允许用户在一个隔离的虚拟网络中提供计算资源，设定局域网，用户可以简便的由自己选择对外开放什么服务，也可以为资料库或较高保安要求的档案设定网络隔离，以虚拟的方式设定私有云中的的网络和系统架构，模拟以单个用户为单位的数据中心。

VPC可以让用户一体化管理架构安全性，提供了安全组和网络访问控制列表等高级安全功能，以便在实例级别和子网级别启用入站和出站筛选功能。－ 容易使用及即时效应,可以通过管理控制台快速又方便地创建及管理VPC，除了有“Start VPC Wizard”来帮助你自动创建范例架构里的子网、IP 范围、路由表和安全组，所作的修改也能立即生效，减省开发成本。使用VPC有很多优点，使用VPC自带的创建功能便可设定公有子网及私有子网，为架构进行完整的网络分离，让网页或APP前端放置在公有子网中开放访问，把资料库，内存缓存服务器等存储用户或商务资料的资源放置在私有子网中保护起来。

用户有自己的数据中心，或自己的本地网络，VPC的directconnect及VPN连接服务能将AWS云服务上的私有网络组合为一个完整的单一网络，简化架构及新服务建设。

**3二三层网络通讯**

传统的三层数据中心架构结构的设计是为了应付服务客户端-服务器应用程序的纵贯式大流量，同时使网络管理员能够对流量流进行管理。工程师在这些架构中采用生成树协议(STP)来优化客户端到服务器的路径和支持连接冗余。

虚拟化从根本上改变了数据中心网络架构的需求。最重要的一点就是，虚拟化引入了虚拟机动态迁移技术。从而要求网络支持大范围的二层域。从根本上改变了传统三层网络统治数据中心网络的局面。

在数据中心网络中，“区域”对应VLAN的划分。相同VLAN内的终端属于同一广播域，具有一致的VLAN-ID，二层连通;不同VLAN内的终端需要通过网关互相访问，二层隔离，三层连通。传统的数据中心设计，区域和VLAN的划分粒度是比较细的，这主要取决于“需求”和“网络规模”。

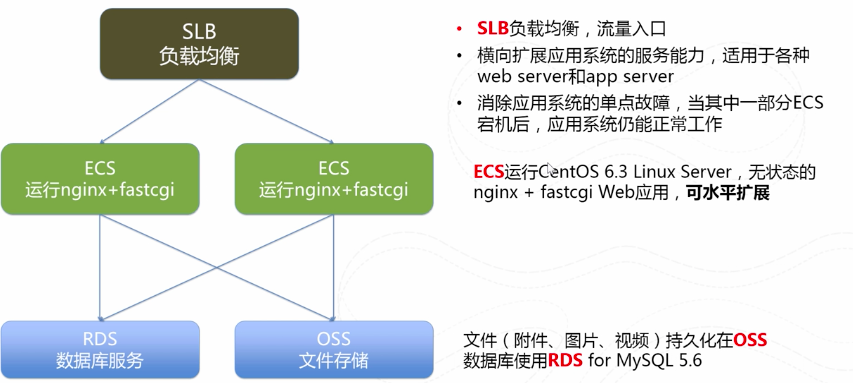
传统的数据中心主要是依据功能进行区域划分，例如WEB、APP、DB，办公区、业务区、内联区、外联区等等。不同区域之间通过网关和安全设备互访，保证不同区域的可靠性、安全性。同时，不同区域由于具有不同的功能，因此需要相互访问数据时，只要终端之间能够通信即可，并不一定要求通信双方处于同一VLAN或二层网络。

传统的数据中心网络技术， STP是二层网络中非常重要的一种协议。用户构建网络时，为了保证可靠性，通常会采用冗余设备和冗余链路，这样就不可避免的形成环路。而二层网络处于同一个广播域下，广播报文在环路中会反复持续传送，形成广播风暴，瞬间即可导致端口阻塞和设备瘫痪。因此，为了防止广播风暴，就必须防止形成环路。这样，既要防止形成环路，又要保证可靠性，就只能将冗余设备和冗余链路变成备份设备和备份链路。即冗余的设备端口和链路在正常情况下被阻塞掉，不参与数据报文的转发。只有当前转发的设备、端口、链路出现故障，导致网络不通的时候，冗余的设备端口和链路才会被打开，使得网络能够恢复正常。实现这些自动控制功能的就是STP(Spanning Tree Protocol，生成树协议)。

由于数据中心内的大二层网络都要覆盖多个接入交换机和核心交换机，主要有以下两类技术。其一就是虚拟交换技术，其二就是隧道技术。虚拟交换技术既然二层网络的核心是环路问题，而环路问题是随着冗余设备和链路产生的，那么如果将相互冗余的两台或多台设备、两条或多条链路合并成一台设备和一条链路，就可以回到之前的单设备、单链路情况，环路自然也就不存在了。尤其是交换机技术的发展，虚拟交换机从低端盒式设备到高端框式设备都已经广泛应用，具备了相当的成熟度和稳定度。因此，虚拟交换机技术成为目前应用最广的大二层解决方案。隧道技术属于技术派。二层网络不能有环路，冗余链路必须要阻塞掉，但三层网络显然不存在这个问题，而且还可以做ECMP(等价链路)，能否借用过来呢?通过在二层报文前插入额外的帧头，并且采用路由计算的方式控制整网数据的转发，不仅可以在冗余链路下防止广播风暴，而且可以做ECMP。这样可以将二层网络的规模扩展到整张网络，而不会受核心交换机数量的限制。

**4弹性负载均衡**

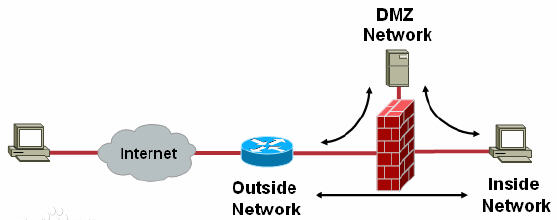
负载均衡它支持将计算任务分摊到多台低配服务器上，然后统一将计算结果返回给客户端。SLB（Sever Load Balancer）是一套软件负载均衡解决方案，它本质上是对多台云服务器ECS进行流量分发，以扩展应用系统对外的服务能力，并通过消除单点故障提升应用系统的可用性。对比硬件负载均衡，它的优势在于低成本、稳定、可扩展、无需运维。运行以太坊节点可用的客户端



一个SLB实例可挂载一个Region下不同Zone的ECS实例，自动实现同城不同机房的容灾。若要实现SLB的容灾，则需要在一个或多个Region创建多于一个SLB实例，通过DNS轮询的方式对外提供服务。SLB提供4层和7层两种负载均衡服务，SLB提供会话保持功能，在session生命周期内，可将同一客户端的request转发到同一backend server上，SLB支持加权轮询WRR、加权最小连接数WLC转发方式，根据后端ECS权重进行转发，SLB针对Https协议提供统一的证书管理服务，证书无需上传后端ECS，解密处理在SLB上进行。

**5安全组和防火墙**

防火墙是依照特定的规则来控制进出它的网络流量的网络安全系统。一个典型的场景是在一个受信任的内网和不受信任的外网比如 Internet 之间建立一个屏障。防火墙可以是电脑上运行的软件，也可以是独立的硬件设备。



与负载均衡器类似，按照其工作的网络层次，防火墙可以分为：

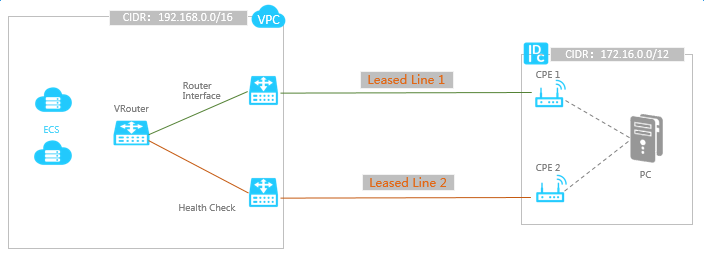
网络层防火墙（四层）：网络层防火墙可视为一种 IP 封包过滤器，运作在底层的TCP/IP协议堆栈上。我们可以以枚举的方式，只允许符合特定规则的封包通过，其余的一概禁止穿越防火墙（病毒除外，防火墙不能防止病毒侵入）。这些规则通常可以经由管理员定义或修改，不过某些防火墙设备可能只能套用内置的规则。 我们也能以另一种较宽松的角度来制定防火墙规则，只要封包不符合任何一项“否定规则”就予以放行。操作系统及网络设备大多已内置防火墙功能。较新的防火墙能利用封包的多样属性来进行过滤，例如：来源 IP地址、来源端口号、目的 IP 地址或端口号、服务类型（如 HTTP 或是 FTP）。也能经由通信协议、TTL 值、来源的网域名称或网段...等属性来进行过滤。

应用层防火墙（七层）：应用层防火墙是在 TCP/IP 堆栈的“应用层”上运作，您使用浏览器时所产生的数据流或是使用 FTP 时的数据流都是属于这一层。应用层防火墙可以拦截进出某应用程序的所有封包，并且封锁其他的封包（通常是直接将封包丢弃）。理论上，这一类的防火墙可以完全阻绝外部的数据流进到受保护的机器里。

安全组是一些规则的集合，用来对虚拟机的访问流量加以限制，这反映到底层，就是使用iptables，给虚拟机所在的宿主机添加iptables规则。  
可以定义n个安全组，每个安全组可以有n个规则，可以给每个实例绑定n个安全组，nova中总是有一个default安全组，这个是不能被删除的。创建实例的时候，如果不指定安全组，会默认使用这个default安全组。

**6.VPN专线**

云专线（Direct Connect）用于搭建用户本地数据中心与华为云VPC之间高速、低时延、稳定安全的专属连接通道，充分利用华为云服务优势的同时，继续使用现有的IT设施，实现灵活一体，可伸缩的混合云计算环境。云专线具有高安全，无缝扩展资源，支持大贷款，低延时的特点。



物理专线由专线和边界路由器组成。每个 IDC 最多可以连接4条专线来搭建冗余物理专线。是一条租用运营商的专线（电缆或光纤），用来连接用户 IDC 至阿里云专线接入点，从而与阿里云 VPC 环境连通。

**7.VPCPeering**

对等连接并非是原生openstack里面的内容。VPC对应OpenStack的一个vRouter及其相关的网络和子网等资源。通常来讲，Neutron的两个vRouter是相互隔离的，才能确保尤其是不同租户之间的安全性，但是在某些场景下存在两个VPC间互通的需求，这种需求的解决方案在AWS里称之为VPC-Peering。

这种使用场景比如：1. 灾难恢复的场景，需要将VPC的数据同步到另一个VPC，实现容灾备份；AWS的VPC现在是不能跨Region的，特定VPC子网也不能跨AZ（Availability Zone），但AWS的VPC-Peering虽不支持跨Region，但支持跨账户；

2. 混合云中尤其是不同云平台的数据间通信时，使用VPC间通信也是可以的，但VPC通信并不是一种标准的通信特性或通信协议，所以会对管理平台或数据模型有一定匹配度要求；

3. 在云平台部署到众多DC规模较小且相互联接的情况下，通过VPC互通为节省用户数据通信的成本；

**8.总结**

通过VPC专有网络，用户可以搭建云上自主可控的网络，自定分配IP地址段、网络规划、子网划分、公网控制、安全控制等；同时，通过使用VPC，用户可以实现云上安全隔离的网络；此外，用户还拥有了更强大的网络功能基础，如带宽包、弹性部署等。

在公网出入控制方面，阿里云提供了EIP、NAT网关、负载均衡控三类产品；此外，阿里云提供的高速通道可以帮助用户实现跨地域/国VPC之间私网互通以及实现云上VPC与云下IDC机房互通的混合云架构。通过这些网络产品，将阿里巴巴拥有全球骨干网的基础设施共享给用户，让用户具备构建企业级全球网络架构能力。

参考文献

1. 阿里云.https://help.aliyun.com/document\_detail/44845.html?spm=5176.110

65259.1996646101.searchclickresult.17eb6f73YNC3jA

[2]sammyLiu. 世民谈云计算https://www.cnblogs.com/sammyliu/p/4658746.html

[3]tursjacky AWS VPC” http://blog.csdn.net/tursjacky/article/details/50517124