Universe Scientific Publishing
Computer System Network and Telecommunications,计算机系统网络和电信(1) 2019,3
ISSN:2661-3719(Print) ISBN:2661-3727(Online)

基于智慧校园的云平台建设方案

杨 健[1] 唐宾徽[2]
四川大学锦城学院 计算机与软件学院 四川 成都 611731

DOI:10.18686/jsjxt.v1i3.1270

【摘要】自1946年世界上第一台电子计算机ENIAC的发明,计算机就开始进入了快速发展的时代。同时随着我国信息化建设的逐步推进,网络技术已经被应用在人们生活、工作中的多个领域,例如高校的网站和各类应用系统的数量急剧增长,导致服务器、存储和网络设备也随之增加,数据中心规模日趋庞大。为解决这个问题,本文从目前的传统校园网络架构来分析和进行缺点描述,并通过对比使用云平台建设新一代的校园网络的优势来说明云平台建设方案的优势和重要。

【关键词】云平台;智慧校园;传统网络架构

1 引言

自1946年世界上第一台电子计算机ENIAC的发明,计算机进入了快速发展的时期[1]。从ARPA-net的建立开始,网络世界开始蓬勃发展。随着我国信息化建设的逐步推进,高校的网站和各类应用系统的数量急剧增长,导致服务器、存储和网络设备也随之增加,数据中心规模日趋庞大。网络中心承担着学校各院部和二级学院的网站与应用系统的管理工作,因此运维管理越来越复杂。为了更加有效地管理这些物理资源,高校在数据中心的建设与管理中逐步引入了虚拟化技术[2],虚拟化平台的建设为数据中心的高效运维以及应用系统的安全管理提出了新思路。

2 传统校园网络分析

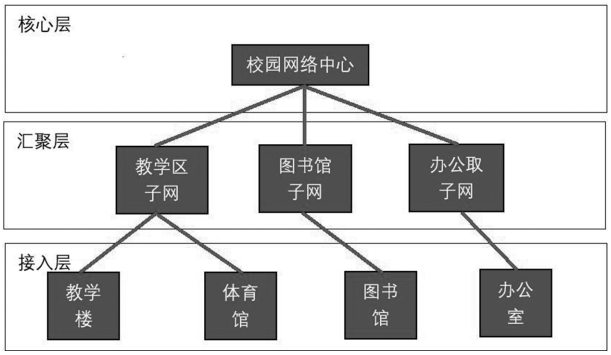
2.1 传统校园网络架构

大型校园网网络系统从设计上分为核心层、汇聚层和接入层;从功能上基本可分为校园网络中心、教学区子网、办公区子网、图书管子网等。目前,先针对传统分层式设计的三个层次进行分析。

(1)核心层:核心层的功能主要是实现骨干网络之间的优化传输。核心层一直被认为是所有流量的最终承受者和汇聚者,是整个网络的核心,所以对核心层的设计以及网络设备的要求十分严格[3]。

(2)汇聚层:汇聚层的功能主要是连接接入层节点和核心层中心。汇聚层设计为连接本地的逻辑中心,仍需要较高的性能和比较丰富的功能,比如负责安全控制等功能。

(3)接入层:在前两个层次的设计中主要考虑的是提供网络性能和丰富网络功能,那么在最底层的设计上主要是提供给最终用户与网络的接口,高速转发所有数据包,提供即插即用的特性。[3]



2.2 传统校园网络的现状

从目前现状看来传统网络架构无法满足学院扩招需求。学校在早期的信息化建设中,已经建有一卡通、教务系统、资产软件、录播、数据平台、Web门户网站、实习等信息系统。但是由于建设时间较早,目前的传统架构的数据中心性能不足,成为了制约学校业务发展的瓶颈[4]。

当前网络数据中心面临的问题:

(1)部分硬件使用时间长,故障率高

学校的一卡通、教务系统应用和数据库、食堂收费系统、门户网站等信息系统的服务器都使用了很长时间,导致设备性能低,无法满足学校每年扩招的系统扩容需求,且该部分服务器设备故障率高,出现故障会导致系统无法运行,影响正常教学。

(2)大量硬件设备导致IT运维管理负荷重

机房内硬件设备过多而且来自不同厂商,同时这些设备也是分散管理,网络、服务器、存储、安全等

ISSN: 2661-3719(Print) ISBN:2661-3727(Online)

设备管理都是相对独立,无法对数据中心内的基础设施进行监控、管理、报告和远程访问。且出现故障时无法及时定位故障点,在故障恢复方面时间较长,维护较难,专业性较高,极大地影响了各业务系统的工作效率,同时也提高了设备成本以及人力成本[4]。

(3)单机单应用、资源利率低、数据丢失风险高

大部分应用都是单机模式,服务器硬件资源分配不平衡。关键服务器资源紧张的同时部分服务器的使用率只有 20%,但剩余的服务器资源不能移为他用,造成服务器资源浪费严重,同时浪费了机房的宝贵空间。

而且数据大部分都是服务器本地存储,如果某台服务器出现故障,相对应的业务也将中断。其次是当硬件需要维护、升级或出现硬件故障时,上层业务系统均会出现较长时间的中断,影响业务的连续性,其中包括一些重要业务系统,一旦中断服务,造成的影响和损失将难以估量[4]。

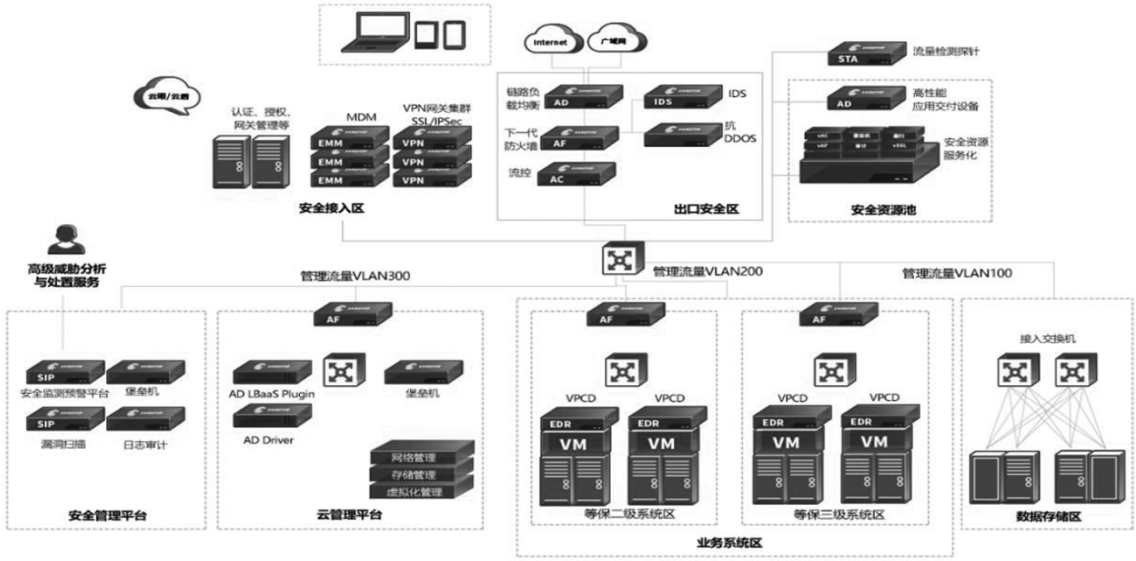
3 云平台的分析

3.1 云平台的类型

云平台顾名思义,这种平台允许开发者们或是将写好的程序放在"云"里运行,或是使用"云"里提供的服务,或二者皆是。

云平台也称为云计算平台,是指基于硬件资源和软件资源的服务,提供计算、网络和存储能力。云计算平台可以划分为 3 类:以数据存储为主的存储型云平台,以数据处理为主的计算型云平台以及计算和数据存储处理兼顾的综合云计算平台。

3.2 云平台的架构



实际环境中的云平台,主要提供三种云服务:

(1)IaaS(Infrastructure as a Service),基础设施即服务。

消费者通过互联网访问云中的计算机基础设施功能来获得服务。这类服务称为基础设施即服务。基于互联网的服务(如存储和数据库)是 IaaS 的一部分。

(2)SaaS(Software-as-a-service),软件即服务

软 SaaS 是一种软件布局模型,其应用完全运行在云中,专为网络交付而设计,便于用户通过互联网托管、部署及接入。供应商的服务器被虚拟分区以满足不同客户的应用需求。对客户来说,相当于购买软件使用权而不是版权,无须在服务器和软件上进行前期投入。对应用开发商来说,只需为大量客户维护唯一版本的应用程序,提供稳定的在线应用。

(3)PaaS(Platform-as-a-Service),平台即服务

平台即服务所谓 PaaS 实际上是指将软件研发的平台作为一种服务,以 SaaS 的模式提交给用户。因此,PaaS 也是 SaaS 模式的一种应用。但是,PaaS 的出现可以加快 SaaS 的发展,尤其是加快 SaaS 应用的开发速度。在 2007 年国内外 SaaS 厂商先后推出自己的 PAAS 平台[5]。PAAS 之所以能够推进 SaaS 的发展,主要在于它能够提供企业进行定制化研发的中间件平台,同时涵盖数据库和应用服务器等。同时 PAAS 可以提高在 Web 平台上利用的资源数量。例如,可通过远程 Web 服务使用数据即服

务(Data-as-a-Service:数据即服务),还可以使用可视化的 API。用户或者厂商基于 PaaS 平台可以快速开发自己所需要的应用和产品。同时,PaaS 平台开发的应用能更好地搭建基于 SOA 架构的企业应用。

3.3 云平台的特征

目前基于云平台业务特性,从云平台边界安全防护、宿主机及虚拟化安全和云管理平台安全出发,在满足合规的基础上,对云平台提供持续保护。因此为满足云平台安全要求,需要子系统具备基线核查、漏洞扫描、访问控制、流量监控、入侵防御、安全加固、虚拟资源隔离等功能,从而实现集成平台和各个安全子系统协助完成云平台安全防护框架[6]。主要有以下六个特点:

(1)全程可视

采用可视化设计,提供多维度安全报表为安全决策提供数据支撑,提供组织安全管理效率。改变了传统的专业工作人员一条条命令配置安全策略的方式,使用户能够清晰的看清资产、业务关系,看懂威胁、安全风险[6];降低了运维难度,也降低了操作门槛,用户可以了解到自己的系统需要什么样的安全策略,从而使用户可以自己配置一些简单策略。让用户明白自己的钱花在了什么地方、做了什么样的工作、对网络安全保护起到了什么作用。

(2 持续检测

对企业核心资产、各类危险与违规行为、网络东西向、南北向流量进行持续检测分析,提高网络整体安全保护能力。持续检测分析可以使用户了解到在什么时刻、什么方式被攻击,是从企业内部人员操作失误还是企业外部黑客病毒攻击,从而合适的调整安全策略,使网络防御更主动。同时当资产的脆弱性风险和网络攻击等安全威胁出现时,可在第一时间发现问题,并于全网海量资产中实现威胁的精确定位。通过平台的大数据分析能力,还原攻击链,对事件进行溯源分析,以便进一步的电子取证,节约企事业单位对通信链路的投资成本。

(3)联动响应

通过防御、检测、响应、云防护、威胁情报的联动,构建本地协同、云端联动的动态保护体系。云端联动:通过虚拟安全组件实现云端全局监测,对所有监测数据进行智能分析,能够及时有效地发现外部攻击行为和云端失陷虚机,并通过可视化报表将分析结果和处置建议发送给云服务用户,从而使用户可以申请相应的安全组件,变更组件规格,修改配置策略等提高网络安全防御。本地协同:通过安全设备之间的智能联动和安全设备与云端之间联动,实现云平台管理配置一键实施,实时更新安全设备的安全策略与状态。实现了针对云环境的体系化安全运营管理平台的安全闭环。所以联动响应不仅能够缩短安全事件的处置时间,避免事件危害的进一步扩散,而且还能提升安全设备的利用效率。

(4)灵活扩展

云平台安全防护可以灵活的提供服务能力,为用户提供基于云安全资源池的安全资源服务,包括负载均衡、下一代防火墙、堡垒机、日志审计等组件,用户可根据业务需求进行安全自管理,使用户建设云业务的同时也避免了安全建设成为固定投入。针对 PaaS/SaaS 等云服务模式,云平台通过基于池化安全资源服务和应用自身的访问控制策略和安全加固措施,共同保障用户业务安全[6]。在云平台安全防护的框架支撑和管理下,多种安全支持手段就可以实施可视化、可管理性、可配置性和智能性的安全保护管理,提供用户按照自我需求灵活高效进行功能扩展的安全保护服务和高度集中操作和维护服务。

(5)全局管控

传统的安全方案缺乏全局的安全检测能力,所以运维人员面对碎片化的安全管理界面,安全运维效率低下,运维难与成本高,最终导致未能及时发现安全风险。如今将设备集成在一起通过安全控制措施统一管理,实现安全管理的配置快速部署和下发,保证设备持续安全运行。通过在各业务区部署流量检测探针,实现对云内资产日志及网络流量的统一采集与分析,构建安全监测预警体系,收集多维信息,帮助用户在云平台上集中和智能的对云内资产、事件统一检测与管理[6]。

(6)减少投入

云平台通过统一管理设备,改变传统安全策略配置方式,降低运维门槛,智能联动响应,远程控制感知事件来下发配置,对事件进行溯源分析,对云业务提供池化安全资源服务等方式降低用户对通信链路的投资成本、云业务成本、人力运维成本、风险成本等。

4 案例对比分析

4.1 校园网络

主要楼宇全部接入校园网,主要分为教学区和宿舍区,增加校园网公网出口带宽管理系统:实现对校园网公网出口流浪的实时监控和必要的流量管

ISSN: 2661-3719(Print) ISBN:2661-3727(Online)

理,确保公网出口的有序、稳定和可控。校园网络主要的特点就是,用户多,信息点多,业务部门多,协同多,网络架构大,数据中心大[7]。

4.2 需求分析

目前校园网再建设的需求大概有:

(1)满足未来五到十年的业务发展的需求及变化

(2)提高校园网的上网速率,提升上网质量

(3)提高访问业务系统的速度,保证业务畅通不间断

(4)保证数据安全性,保证访问高峰期不宕机

(5)建设集中管控,可视化的运维管理方式

4.3 架构优势对比

(1)传统网络架构模式

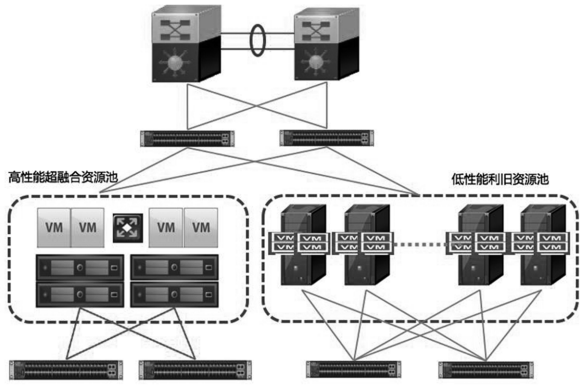
如果使用传统网络架构思路:1)使用传统的路由器独立计算路由方式;2)更多设备搭建新环境形成更大的二层架构;3)仍通过核心层转发业务;4)传统运维人员手工配置命令

会导致的结果:1)网络延迟大,网速仍然慢;2)负载均衡利用率低;3)增加新业务模块困难,不能满足未来发展需求;4)运维困难,运维成本高;5)校园宽带有限,主干链路冗余能力弱,修改难度大。

(2)云平台架构模式

云平台架构思路:1)采用新型超融合架构,高性能资源池承载核心关键应用,利用旧资源池承载非关键业务;2)基于云安全资源池等构建池化的安全资源服务提供负载均衡;3)基于安全感知平台和流量探针,构建安全监测预警体系,实现云安全全局监测和统一管控;4)通过虚拟化技术,将计算、存储、网络和网络功能(安全及优化)深度融合到一台标准X86服务器中,形成标准化的超融合单元,多个超融合单元通过网络方式汇聚成数据中心整体IT基础架构,并通过统一的WEB管理平台实现可视化集中运维管理;5)核心交换节点采用VSS技术,提高流量负载均衡可靠性;6)优化网络路径[8]。

云平台架构下的效果:1)整合了校园分散的IT硬件资源,提高资源利用效率;2)节约机柜、机房空间占用;3)并实现IT资源模块化建设和横向弹性扩展能力,加速学院业务需求响应速度,缩短IT基础设施资源的交付周;4)提高运维效率,降低运维门槛;5)降低宕机风险,提高业务连续性;6)所有业务系统均迁移至云平台并稳定运行,不存在单机单应用、数据本地存储存在的风险[9]。



在云平台架构建设中,采用了超融合技术,解决了传统网络架构中网络利用率低,设备维护困难,流量负责均衡难以起效等问题[9]。该技术方案的优势是:1)整合旧有资源,节省校园IT建设成本;2)打造智慧校园,未来业务扩展更方便;3)统一管理,全局管控,维护方便,全程可视

5 结束语

总而言之,云平台可以为现在的校园建设提供很多帮助,满足用户实际需求也满足用户未来几年的发展需求。云平台的功能多种多样,我们也看到了其在网络优化方面的便捷之处,其重要性和必要性也不言而喻,所以需要大力支持发展。

【参考文献】

[1]史宝虹.高校虚拟化数据中心平台建设及迁移研究[J].电脑知识与技术,2018,14(21):15-17.
[2]康靖.计算机技术应用领域及其发展展望[J].科技创新与应用,2014,(1):70-70
[3]金路.基于云计算下计算机信息安全与保密分析[J].网络安全技术与应用,2019(05):32-33.
[4]黎剑鸣.大数据环境下的智慧教育云平台构建研究[J].科学技术创新,2019(20):77-78.
[5]左明慧.基于GPON的高校校园网扁平化架构设计研究[J].价值工程,2018,37(35):251-253.
[6]李磊.浅谈如何构建云平台安全的防护体系[J].网络安全技术与应用,2019(07):66-67.
[7]王爱彬.构建云平台安全的防护体系与手段[J].通讯世界,2018(09):35-36.
[8]章玮.无线校园网的安全架构研究与设计[D].云南大学,2014.
[9]胡进娟.高校虚拟化平台建设方案研究[J].电子元器件与信息技术,2018(10):27-29.