云环境的校园网数据中心安全策略①

葛苏慧[1], 梁宏涛[2], 房正华[1]

[1](青岛工学院 信息工程系, 青岛 266300)
[2](中国海洋大学 信息科学与工程学院, 青岛 266100)

摘 要: 在校园网安全策略中, 传统的高校数据中心仅把流量安全当作考虑因素, 而云计算环境下虚拟化数据中心的安全模型则由二维变为三维, 本文提出了四种安全策略, 并设计了云环境下的校园网数据中心安全与设备部署, 从而提高云环境下的校园网数据中心安全.

关键词: 云环境; 数据中心; 安全策略

Campus Data Center Security Policy in Cloud Environment

GE Su-Hui[1], LIANG Hong-Tao[2], FANG Zheng-Hua[1]

[1](Information Engineering Department, Qingdao Institute of Technology, QingDao 266300, China)
[2](Information Science and Engineering College, Ocean University of China, QingDao 266100, China)

Abstract: In the campus network security strategy, the traditional data center consider the counted traffic safety as the only factor, but virtualized data center security model in cloud computing environment is changed from 2 d to 3 d, this paper puts forward four kinds of safety strategy and design the campus data center safety and equipment deployment in the cloud environment, in order to improve the campus data center security.

Key words: cloud environment; data center; security policy

1 引言

随着云技术的飞速发展, 利用虚拟化技术的数据中心, 整合了服务器、存储和网络等各种物理资源, 实现弹性云服务模式, 将为传统校园应用提供多种云服务平台, 包括数据存储云服务、科研计算云服务、桌面虚拟化云服务等. 尽管有纵向和横向两种安全策略, 传统高校数据中心在校园网的安全策略上都是把流量安全当作仅有的考虑因素, 但为适应新技术, 云环境下虚拟化数据中心的校园网安全模型应该有所变革, 需增加另一维空间的安全策略, 由二维平面转化为三维立体, 达到授权之后主机加入或离开计算集群、虚拟机动态迁移、隔离大量用户之间的多种业务等, 但这些功能传统的数据中心是无法实现的. 安全作为云环境中的一种服务, 怎样适应基础的网络架构及虚拟化的应用服务, 实现虚拟交付, 是校园网安全策略关注的重点. 要解决以上问题, 基于云环境的虚拟化校园网数据中心安全建设必须借鉴新思想和新方法, 如扩展虚拟局域网、安全策略上移、安全策略随着虚拟机动态迁移等.

2 云环境的校园网数据中心安全策略

2.1 VLAN 扩展

虚拟化校园网的数据中心作为集中资源对外服务, 面对成倍增长的用户, 承载的服务是海量的, 尤其是面向公众用户的运营云平台, 应允许师生、家长及校外用户随时随地从任意终端访问校内的公开服务信息资源, 使学生的学习不再局限于学校机房或教室, 而是在任意地方都可登录到校园网络获取构建学习环境的资源和服务, 增强网络学习的灵活性和敏捷性, 实现学习资源的“按需而用, 即需即用”. 同时家长能及时掌握学生的学习状态, 社会能全面了解学校的发展现状. 所以, 云平台(虚拟逻辑机或物理机)的安全性、

① 基金项目:2013 年山东省高校科技计划项目(J13LN78)
收稿时间:2013-08-19;收到修改稿时间:2013-09-24

可靠性, 以及该平台海量用户、各种业务之间的清晰的隔离和安全识别, 都是数据中心的管理人员需要考虑的因素. 要标识和隔离大量用户, 对于基于云环境的各个用户最好的方法是为他们提供不同的 VLAN ID, 但可提供的虚拟局域网的数量最多是 4096 个, 云环境下的大量业务无法进行, 所以需要扩展 VLAN[1].

因为云拥有灵活、动态、弹性、敏捷、随需应变的特征, 因此需要一个灵活、动态、弹性的架构作为云计算的基础. 考虑支持虚拟化的防火墙, 是网络基础设施角度的必然选择, 不同的用户可以基于 VLAN 映射到不同的虚拟化实例, 每一个虚拟实例有独立的安全控制策略和管理功能[2]. 图 1 为使用 VLAN 技术把不同的用户映射到不同的虚拟化实例中.

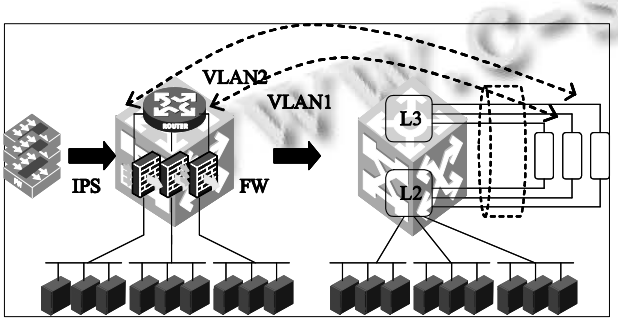

图 1 基于 VLAN 不同用户映射到不同的虚拟化实例

2.2 安全部署边界的选择

传统校园网安全保护策略中的基本原则是, 不同的区域采用不同的策略, 即所谓的依靠边界的隔离和访问控制策略, 但这种方法要由区域之间事先划分的边界为基础. 但是在云计算的环境中, 统一了基础的网络架构, 实现了计算和存储资源的高度融合, 因此安全设备之间的部署边界全然消失, 这将意味着安全设备的部署方式不再像传统的安全建设模式, 基于云计算环境中的安全部署需要寻找新的模式.

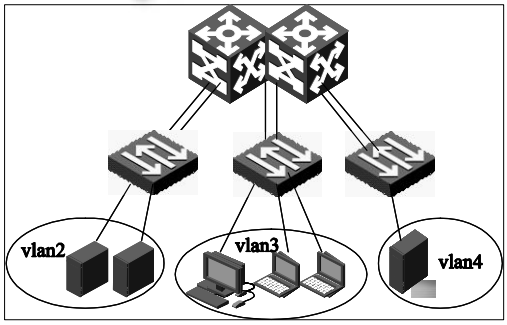

图 2 安全部署边界的选择

使用 IRF2 策略的汇聚交换机是第二层和第三层的分界点, 校园内的服务器属于三层模式, 而面向网络的一方属于二层模式, 这就是数据中心浏览器/服务器的工作特点. 校园内各种不同的服务, 如 Web、AP、DB 等, 对应一定的 VLAN, VLAN 之间的互访通过 ACL 来控制, 各种服务与外界通过防火墙实现安全控制, 并由三层汇聚交换机作为网关, 控制进出的数据流[3]. 防火墙和交换机都会对虚拟路由转发表进行划分, 把统一的业务划分到同一个 VRF 内, WEB/AP/DB 则划分到同一 VRF 不同的二层分区内[4]. 交换机的三层路由功能实现同一业务 Web、AP、DB 之间的通信, 使用 ACL 对访问业务进行控制; 通过跨 VRF 防火墙实现不同业务之间的通信. 其次, 校园内三层接口对应的网络需经防火墙访问另一个网络时, 可以配置一条“弱策略路由”, 这条路由的下一跳为防火墙, 防火墙是否正常工作决定了这条路由的正常使用, 因此可以配备一个旁路防火墙, 从而保证这条路由的正常运行[5]. 这种方法适用于基于虚拟化环境的虚拟机的迁移, 并且使用交换机的访问控制列表 ACL 来隔离不同的应用, 相对于频繁调整的客户机是一个较好的应对方法, 所以适合在安全隔离要求较低、主机部署灵活性较高的环境中使用[6].

2.3 集中的安全服务中心

传统的安全建设模型注重不同的边界防护策略、存储资源和计算资源的高度集成, 所以校园网内的不同用户申请云计算的服务时, 只能实现逻辑上的隔离, 不可能有物理上的安全边界. 因此, 按照校园网用户的分类来汇聚用户流量和部署独立的安全边界系统将不再可能. 所以基于各子系统安全防护的服务部署应该转变成对整个云计算环境的防护, 建设集中的安全中心, 来适应物理模型的逻辑隔离[7]. 云服务提供商或云管理员能够经过适当的方法把要求安全服务的用户流量引入到集中的安全服务中心, 待完成该安全服务之后再重新返回原来的转发路径. 安全服务中心的集中, 不但能够完成用户安全服务的单独配置, 而且能够节省建设成本. 在一定收敛比上提供安全服务的部署图如图 3 所示.

2.4 云安全模式的耦合

最大程度上使用校园网内云端强大的计算力来实现云模式的安全检测及防护, 是校园网一个重要的发

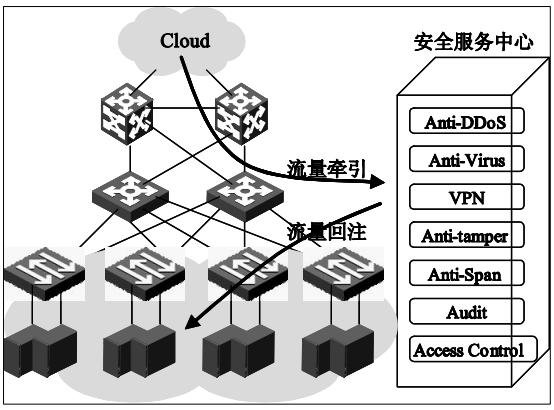

图 3　集中的安全服务中心部署

展方向. 相对于传统的安全防护模型, 云环境下的安全模型不仅要求云端海量的本地客户具有基本的威胁检测及防护功能, 更强调他们对未知或可疑威胁的传感检测能力[8]. 对于不能正确判断的可疑流量, 校园网内的用户可以将其送至云检测中心, 云端高速准确的检测能力可以正确定位并解除威胁, 还可以把这些可疑流量的数据特征发送给所有客户, 甚至网关, 让云中的客户和网关都具备检测这种未知威胁的能力, 从而真正实现客户模式建立的安全防御体系中的安全闭环 PDRR(Protection, Detectiong, Reaction, Restore)策略[9]. 如图 4 所示, 这也是云检测模式的精髓所在.

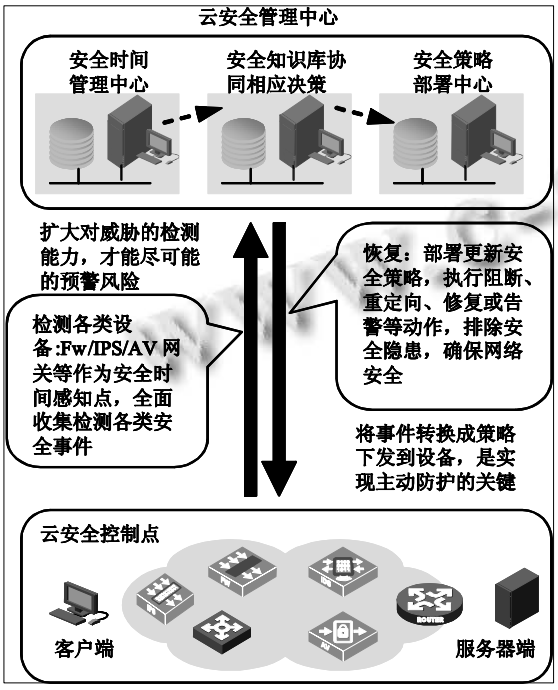

图 4　云安全模式管理示意图

3　校园网数据中心安全设计

在云环境的校园网数据中心安全的建设中, 简单的图框只能表达逻辑拓扑结构, 不能满足数据通信的安全设计. 因此需要全方位综合考虑, 包括机房建设标准、业务应用模型等. 以下采用 TIA-942 标准来设计校园网数据中心机房的设备、结构模型及网络部署, 因此需满足以下需求: 数据中心服务器数量 500 台, 服务器千兆双网卡接入, 服务器接入交换机通过万兆级联到汇聚层交换机, 每台服务器功耗 300W, 每个网络机柜最大功耗 3kW, 每个存储机柜最大功耗 2kW, 存储网络有单独的机柜[10].

3.1　逻辑拓扑

根据校园网的应用需求, 所有业务可以分为 Web、AP、DB 三个逻辑访问区, 每个区域都是标准的三层模型, 接入层使用 H3C 的 S7510E 设备, 汇聚层使用 S9512E 设备, 核心层使用 S12508 设备. 这种扁平的组网结构改变了以前依据应用“糖葫芦串”式的划分方法, 将最大限度的满足海量用户的访问需求, 便于校园网数据中心机房的可扩展性[11]. 校园网数据中心如图 5 所示, 客户端访问数据中心通过专用的 FW 处理, 提高数据中心的对外安全, 在校园网内部, 各种信息之间的相互访问由数据中心汇聚层的 FW 来控制, 从而提高安全性[12].

在 Web、AP、DB 三个逻辑访问区内放置 4 台 S7510E 设备连接服务器, 每台 S7510E 通过 2*10GE 捆绑链路级联到汇聚层, 并配置 2 块 4*10GE 单板. 汇聚层使用 S9512E 设备, 部署 FW 插卡, 提高安全性. 基于 Web 区域的应用类型, 负载均衡功能必不可少, 因此需要在 Web 区的 S9512E 上配置 LB 插卡, 使用 2*10GE 级联到两台核心汇聚交换机 S12508 上, 使用 4*40GE 与汇聚层同一区域另一台 S9512E 相连, 使用 4*10GE 与接入层的 S7510E 互联. 核心层放置 2 台 S12508, 每台使用 2 块 4*10GE 单板, 通过 3*10GE 与另外一台 S12508 互联, 通过 2*10GE 与汇聚层的 S9512E 互联, 满足各层业务之间的通信.

3.2　网络安全与设备部署

部署校园网数据中心要依据业务不同级别的重要性, 从安全和应用考虑, 将网关设置在不同的设备上. 业务访问模式分为两种类型: 纵向访问是同一种业务在不同区的访问; 横向访问是同一级别中不同应用之间的访问[13]. 根据应用需求, 区分业务级别, 部署方

案如图 6 所示.

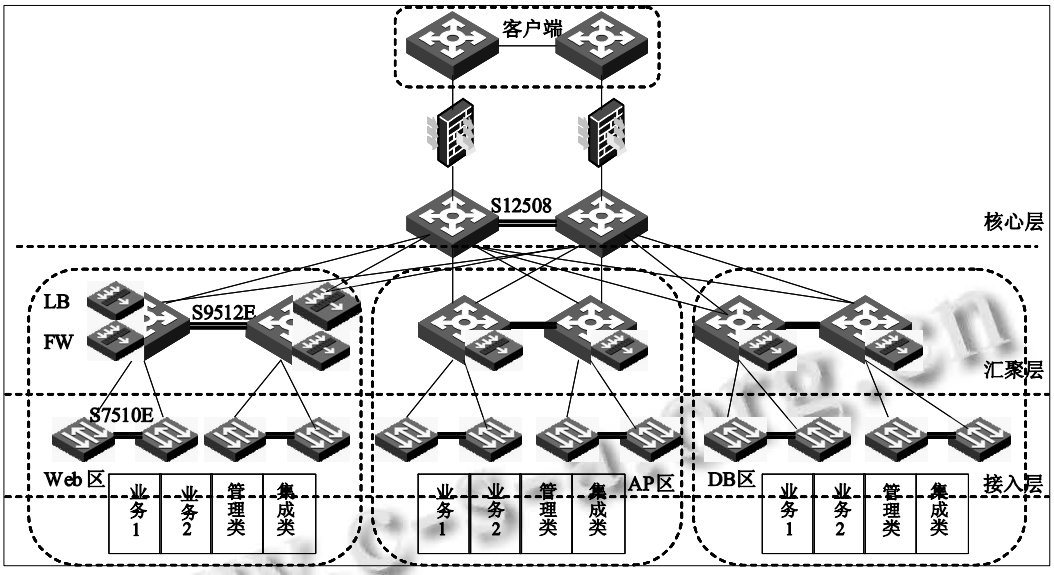

图 5 校园网数据中心拓扑

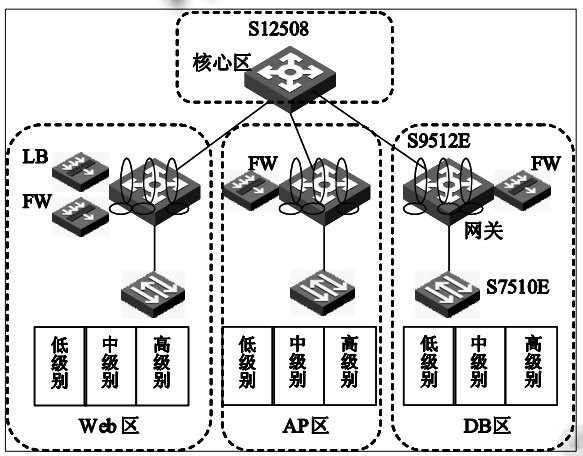

图 6 数据中心安全部署

低级别的应用服务, 在汇聚层交换机 S9512E 上设置网关, 并通过 ACL 访问控制策略实现纵向、横向访问; 对于中级别的应用服务, 横向访问使用交换机 ACL 访问控制列表实现, 纵向访问通过防火墙控制; 而高级别的应用, 横向和纵向访问都要由防火墙来控制[14]. 针对以上三种业务的虚拟化, 可使用 MCE 技术并绑定 VPN 实例实现相互之间的业务隔离, 将大大减少 ACL 配置和资源损耗. 服务器之间的二层交换由接入层 S7510E 控制, 汇聚层 S9512E 与 FW 互通, 并实现与核心层 S12508 跨区域的路由转发, 核心层 S12508 交换机控制不同区域业务之间的通信.

4 结语

云环境下的校园网安全将是高校信息化发展的重要因素, 作为最底层的基础平台会遇到很多挑战, 一方面改善现在的技术来优化以往的安全模式, 另一方面应不断采用新技术来迎接挑战. 进一步探索新的安全模型, 在云环境的数据中心基础网络架构中嵌入安全策略, 采用更加安全的交互方式, 提高了云环境下校园网数据中心的认证鉴别能力, 并且可提供实时的控制策略, 从而避免传统安全策略的弊端, 大大提高云环境下的校园网数据中心安全.

参考文献

1 Cook G, Horn JV. How dirty is your data? A look at the energy choices that power cloud computing[Technology Report]. Greenpeace International. April 2011.

2 Qureshi A. power-demand routing in massive geo-distributed systems [PhD Thesis]. Massachusetts Institute of Technology, 2010.

3 Gao PX, Curtis AP, Wong B, Keshav S. It’s not easy being green. Proc. of the ACM SIGCOMM 2012. Helsinki, Finland. 2012.211–222.

4 杭州华三通信技术有限公司.新一代网络建设理论与实践. 北京:电子工业出版社,2011.10.

(下转第 152 页)

各自均处于波动状态. 由于 node3 距离接收基站比较近, 所以其传输率一直相对很好. node0、node1、node2 和 node3 平均的吞吐量分别是: 0.1996Mps、0.1848Mps、 0.1926 Mps 和 0.4969 Mps.

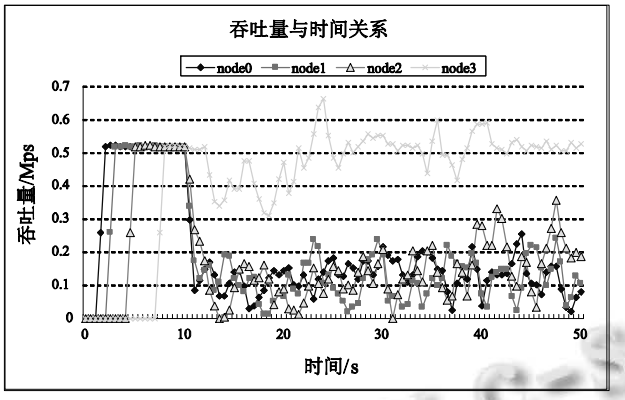

图 5 吞吐量与时间关系图

上面的数据分析结果给现实搭建应用系统提供了理论依据. 在实际的系统构建中, 要针对应用的需求, 放置节点的位置, 节点的位置不同将影响数据传输的效果和质量, 决定数据的正确性.

6 结论

文章针对火车头监控系统的特点, 采用分层结构对火车头车位监控系统进行建模, 并根据系统的应用需求应用了 DSDV 路由协议. 根据仿真结果得出结论, 此模型所有数据都起于无线节点, 并通过基站, 终于服务节点. 仿真的场景与实际中的监控场景类似, 符合系统的监测要求. 后续研究工作重点是开发更有效的路由协议, 搭建实际的系统, 应用于实际地系统监测.

参考文献

1 刘媛媛,朱路,黄德昌.基于 GPRS 与无线传感器网络的农田环境监测系统设计.农机化研究,2013,(7):229–232.
2 李娜,马向阳,钟志良等.基于无线传感器网络的天然气工业安全监测.仪表与自动化,2013,31(2):79–83.
3 司海飞,杨忠,王珺.无线传感器网络研究现状与应用.机电工程,2011,28(1):18–20,37.
4 刘利强,王岳斌.无线网络路由协议性能的研究与仿真.电子技术,2013,(2):9–11.
5 王北光,李立新,谢涛.移动 Ad Hoc 网络 DSR 协议的改进.计算机技术与发展,2011,(8):121–128.
6 李琼,张亮.基于 NS2 的 AODV 路由协议仿真及分析.计算机与现代化,2012,(7):79–82.
7 王立新,赵元庆,谷川.WIA-PA 中基于 DSDV 的多路径路由协议研究.计算机工程与设计,2011,32(10):3338–3341.
8 曾文丽,裴廷睿,张朝霞等.混合无线 Mesh 网络中改进的分层 AODV 路由协议.计算机工程与应用,2010,46(19):125–128.
9 周莉,张燕,许璐蕾等.Ad Hoc 网络路由协议 DSDV 的仿真研究与实现.福建电脑,2012,(11):93–95.

(上接第 215 页)

5 徐笑宇,黄磊.虚拟化技术在高校信息化建设中的探讨.西南民族大学学报(自然科学版),2011,34(4):818–822.
6 Joysula V, Orr M, Page G. 张猛译.云计算与数据中心自动化.北京:人民邮电出版社,2012.
7 师雪霖,徐恪.云虚拟机资源分配的效用最大化模型.计算机学报,2013,(2):252–262.
8 秦秀磊,张文博,魏峻等.云计算环境下分布式缓存技术的现状与挑战.软件学报,2013,24(1):50–66.
9 张廷伟.云管理从数据中心管理开始.IP 领航,2010,(4):121–123.
10 宋雨,易璐,王凤霞.基于云存储的重复数据删除架构的研究与设计.计算机系统应用,2013,22(1):208–211.
11 刘晓茜,杨寿保,郭良敏.雪花结构:一种新型数据中心网络结构.计算机学报,2011,(1):76–86.
12 邓维,刘方明,金海.云计算数据中心的新能源应用:研究现状与趋势.计算机学报,2013,(3):582–588.
13 叶可江,吴朝晖,姜晓红,何钦铭.虚拟化云计算平台的能耗管理.计算机学报,2012,(6):1262–1285.
14 冯等国,张敏,张妍等.云计算安全研究.软件学报,2011,22(1):71–83.