数字校园网络立体化安全防护的研究

蒋建军[1,2]

(1. 上海电机学院 网络信息中心,上海 200240;
2. 武汉理工大学 信息工程学院,湖北 武汉 430070)

摘 要:校园网络安全隐患很多,对高校教育信息化应用带来了诸多不便,数字校园的安全需要综合考虑信息安全管理、物理安全、网络安全、主机安全、应用安全等多方面的因素,因而迫切需要建立一个立体化的安全防御体系。文中介绍了数字校园立体信息安全的建设思路,详细分析了内控外防、认证相辅的实现技术和外网出口的安全防御方案,在重点业务核心区域采用层次防御、审计相随的层次化安全防范技术。在多校区管理中,实现整网延伸、安全可信的校园网络信息安全建设原则,构建了按区域、分层次的多校区校园网稳定、安全的体系架构。实现了整体的立体安全防护效果,实践效果达到了网络信息安全的防护作用。

关键词:校园网;信息安全;认证;审计;立体化;安全防护
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2015)09-0159-05
doi:10.3969/j.issn.1673-629X.2015.09.034

Research on Digital Campus Three Dimensional Network Security Protection

JIANG Jian-jun[1,2]

(1. Network Information Center, Shanghai Dianji University, Shanghai 200240, China;
2. School of Information Engineering, Wuhan University of Technology, Wuhan 430070, China)

Abstract: Many campus network security risks bring a lot of inconvenience for information technology applications in education college, digital campus security needs to take various factors into account including information security management, physical security, network security, host security, application security, and thus it is an urgent need to establish a three-dimensional security defense system. In this paper, introduce the three-dimensional digital campus information security building ideas, detailed analysis of implementation techniques of the internal control and external defense, certification complementary and external network security defense export program, the focus of the core business area using hierarchical attendant prevention technology with hierarchical defense and security audit. In multi-campus management, the realization of the entire network extension, safe and reliable campus network information security principles, construct a regional, multi-tiered architecture of campus network with stability and security. Achieve the overall three-dimensional defense effects, practice effect reaches the protection purpose for network information security.

Key words: campus network; information security; certification; auditing; three-dimensional; safety protection

0 引 言

中国的高校信息化已经开展了将近二十年,与其他行业一样,数字化校园的基础架构随着 IT 技术的不断发展,逐步走向融合、虚拟化,真正开始面向以应用为核心提供灵活扩展的服务平台。高校的新一代数据中心的建成将为学校师生提供一流的数字化校园生活,为实现学校办学目标提供了信息化保障。

随着数据校园网传输数据类型越来越多、数据量越来越大、数据的重要性持续提高,如何提升数据传输、数据处理、数据应用的安全性,需要综合考虑信息安全管理、物理安全、网络安全、主机安全、应用安全等多方面的因素[1]。如何建设一个高效的校园信息安全体系,成为学校信息化建设思考的重要问题。

为实现这一目标,在信息化建设过程中应采用立体安全防护新理念,建成的新一代数字化安全校园体系架构,可为学校的网络安全打下良好的基础。

收稿日期:2014-10-27 **修回日期**:2015-01-27 **网络出版时间**:2015-08-26
基金项目:上海市科技计划基金项目(14511108003)
作者简介:蒋建军(1967-),男,副教授,高级工程师,研究方向为计算机网络与教育、信息技术。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20150826.1535.020.html

1 校园信息安全建设总体目标

将信息安全作为一个整体来考虑时,数字校园的安全建设从三个部署层面(如图 1 为校园网立体安全建设总体策略图),实现校园网、数据中心访问的事前认证策略、事中控制体系、事后追溯机制,有效保障全校信息化的整体安全。

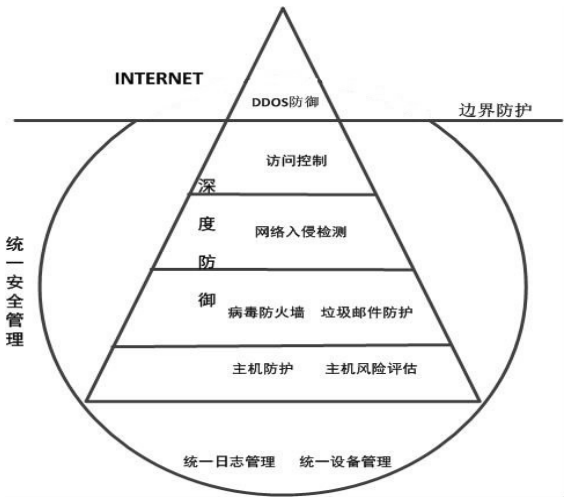

图 1 校园网立体安全建设总体策略

(1)边界防护。

局域网出口端的安全防护,充分考虑学校校园网在 DDoS[2] 攻击防范、P2P[3] 控制、5-7 层攻击防护的实际需求。通过 IPsec VPN[4] 技术,实现新老校区间 VPN[5] 互联,作为裸光纤的备份链路,能保障新老校之间互联的高可靠性。

(2)内部深度防御。

核心业务服务器区域,对 Internet 访问的二次防护,增强系统安全性;对内部用户,通过防火墙的实现策略细分控制,强大的虚拟防火墙功能,有效保障了各个区域的安全性。

(3)统一安全管理。

主要包括局域网内部的统一日志收集功能,对校园网的各个系统的日志集中采集,及时发现威胁,并构建事后审计机制。

2 系统核心技术与创新

校园网网络安全建设,本着校园网信息安全建设业务保障、技术创新的原则实现:内控外防、认证相辅;层次防御、审计相随;整网延伸、安全可信。

2.1 内控外防、认证相辅

校园网网络安全建设总体设计办法采用“内外结合”的方法来实现。一般情况,网络威胁的来源主要来自于内网威胁和外网威胁两种。内网威胁主要分为非法使用网络和非法的网络攻击行为[6],而外网威胁则来源于 L_2-L_7的互联网攻击和非法言论。

根据不同的威胁根源,校园网的安全设计分两种情况实现。第一情况是解决内网安全,用入网即认证的方式来解决非法用户接入的问题。具体可通过一台认证服务器来实现整个校园网的认证,所有访问校园网的用户首先必须通过认证。

实现技术如下:校园网的接入层交换机作为 802.1X 的接入认证设备,负责对 PC 客户端的接入控制,城市热点设备作为 802.1X 的认证授权 Raduis 服务器,来为认证通过的用户分配接入网络的权限(如图 2 为接入认证拓扑结构图)。认证失败的用户将无法接入校园内网,认证失败的交换机端口只能传输认证协议报文,无法传输其他数据报文,从而达到安全接入管控的目的,非授权用户无法随意接入校园网络。

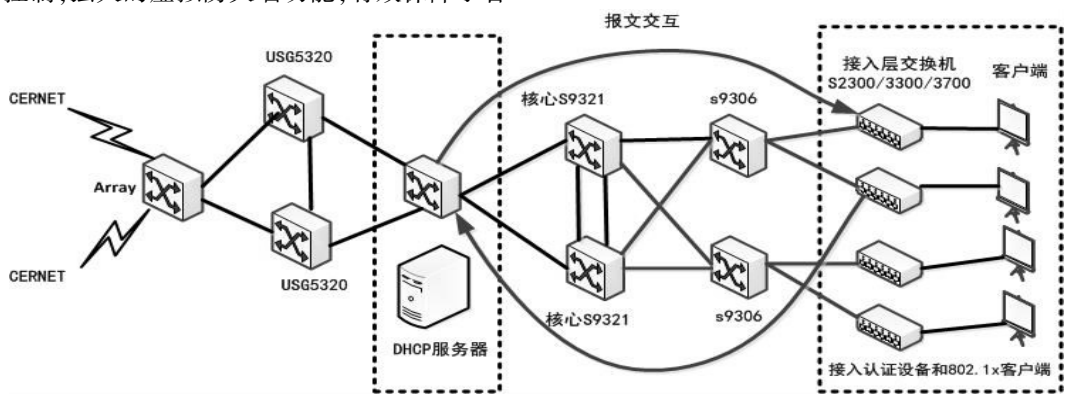

图 2 接入认证拓扑结构图

第二种情况是解决外网安全威胁。校园网互联网出口是内网与外网的唯一接入点,所以在互联网出口需要部署切实可行的网络安全防御体系。方法是在出口部署两台冗余的高性能统一安全管理设备,主要实现 L_2-L_4的安全防御,同时支持 L_5-L_7的应用层防御。同时核心交换机部署的 IDS[7] 设备,实现全网进出流量威胁检测,通过策略同前端防火墙联动,完善防御体系。

校园网的外网出口承担着入侵和攻击防范的重担,因此需要建立 L_2-L_7的安全防御体系,并对进出的流量进行分析统计,以便运维人员更好掌握业务分类及使用情况;防火墙和 IDS 的联动进一步加固安全防

范能力。

图 3 为外网出口安全防御拓扑图,即入侵检测加统一安全网关,实现的关键技术如下:

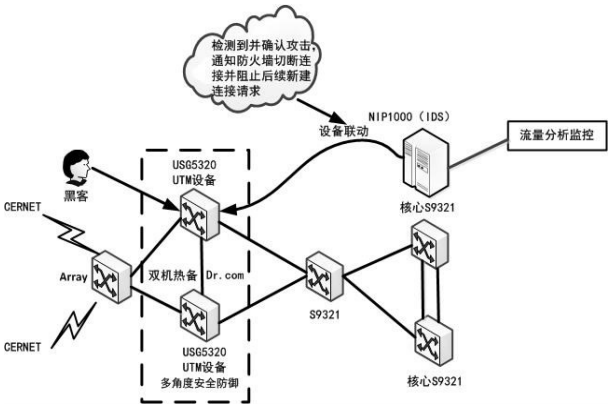

图 3　外网出口安全防御拓扑图

1)IDS 实现技术。

IDS 采用全面的检测技术:

(1)采用协议智能识别技术,自动区分不同应用和协议,无需人工设定协议端口;

(2)基于漏洞的检测技术,以及基于攻击特征的检测技术,实时发现并防御各种已知的攻击:漏洞利用、蠕虫木马等等;

(3)协议异常检测、流量异常检测以及启发式检测技术,可以有效地发现未知漏洞及恶意软件产生的攻击;

(4)NIP 产品荟萃多种入侵检测技术,其中最重要的就是基于漏洞的检测,可有效地阻止因为漏洞而带来的威胁,如:溢出攻击、蠕虫感染等。相对传统的攻击特征检测不会产生误报,并且能够更好地对抗使用逃避技术的攻击行为。

2)UTM 实现技术。

运用 USG5300 严格的安全策略控制以及 DDoS 的攻击防护能力,辅以 UTM 的统一威胁管理功能,完善校园网出口的多维度安全防御。

2.2　层次防御、审计相随

数字校园网络的建设,充分考虑各种用户和数据的安全性。通过安全域策略和层次化建设来实现高效的安全。

在关键的核心业务服务区,部署华为公司具备万兆性能的分布式 ATCA 架构的 USG9100 防火墙,接入示意图如图 4 所示。实现对该区域的二次防护,有效阻断外部 Internet 网络对核心业务服务区的访问,实现对校园网内部用户对该区域的访问控制,实现业务区域的按需访问[8]。

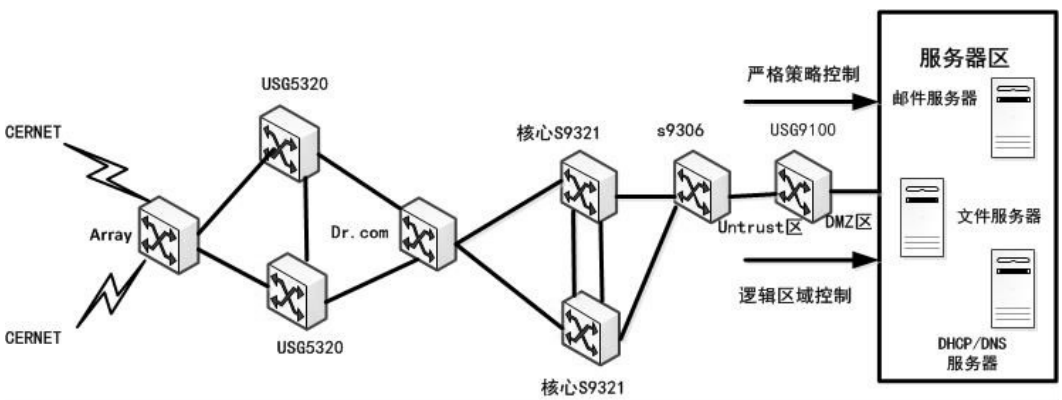

图 4　防火墙接入示意图

针对核心主机、数据库、网络设备等的日志管理及运维审计,通过目前的 eLog 日志审计系统和 UMA 统一运维管理设备来实现。eLog 日志管理系统通过高效地采集网元的日志,管理员能及时了解安全网元、网络网元、主机服务器和数据库服务器的运行情况,了解网络用户的行为,迅速识别并消除安全威胁。统一运维审计(Unified Maintenance Audit,UMA)提供统一的运维操作入口,控制并记录用户进行的运维操作,支持以命令查看、视频回放等方式进行审计。

1)防火墙的安全策略及攻击防范技术。

(1)通过划分不同的逻辑安全区域实现安全策略隔离,例如 Untrust、DMZ、Trust 等等。

(2)不同安全区域之间应用严格的安全策略,针对不同主机的 IP 和 TCP/UDP 的端口号进行策略的放行,没有策略允许的数据流是被严格拒绝的。

(3)通过开启 DDoS 防御功能,保护服务器不受大流量的冲击,正常为校园网用户提供优质服务。

2)UMA 统一运维审计系统技术的实现方式。

(1)统一运维入口:为校园网核心业务系统提供统一维护操作入口,实现单点登录。

(2)集中帐号管理:实现自然人与设备帐号之间的一一对应,并提供定期密码修改功能。

(3)严格权限控制:为不同运维人员分配不同的权限,实现命令级的控制,确保合法用户对资源的操作,杜绝越权访问。

(4)安全审计:记录所有运维操作过程,快速的故

障定位和责任追踪;并为第三方审计机构提供审计报表和原始日志。

(5)多种方式运维:支持字符终端、图形终端、数据库、应用终端、文件传输以及 KVM 运维方式。

由于校园网络及业务系统的庞大,难免出现针对主机系统、数据库的安全事件。例如后门木马、内部人员篡改数据等[9],如何及时发现并制止这类安全事件呢? 针对可能出现的问题,部署一套完善的日志管理和安全审计系统,有效实现对全网日志的全面收集和及时审计。

2.3 整网延伸、安全可信

目前,许多高校新建了新校区,对于新校区建成后,如何实现新校区同老校区的安全、高速互联,成为摆在面前的一个现实问题。通过裸光纤的形式,实现了新老校区核心交换机之间的高效互联。但是,由于新老校区之间业务交互频繁,交互数据量较大,为了保证新老校区之间连接的高可用性,部署 SVN3000 来实现新老校区通过 IPsec VPN 的安全互联,作为裸光纤的备份网络,保障了学校整体网络的高可用性。

两个校区的核心交换机之间通过裸光纤高速连接,考虑到两个校区通信频繁,不能容忍长时间链路中断,因此通过 SVN3000 专业级的 VPN 网关来实现两个校区之间的链路容灾备份。图 5 所示为 SVN3000 互联示意图。

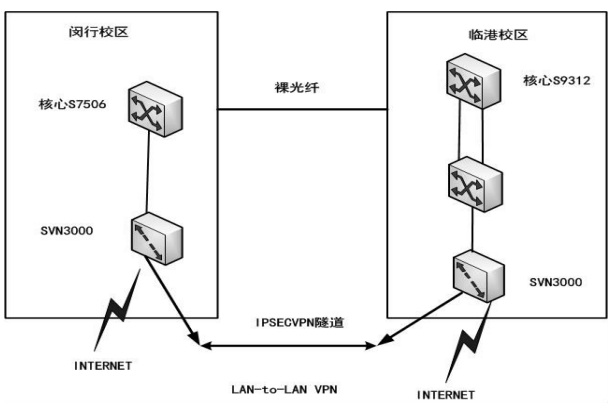

图 5 SVN3000 互联示意图

VPN 备份链路实现方式:

(1)日常两个校区通信,数据直接在核心交换机上路由转发。

(2)当两个校区裸光纤故障断裂后,两个校区之间的 OSPF 路由从 OSPF 路由表内消失,提前配置在核心交换机上的浮动静态路由生效,数据将会走到 SVN3000 上,从而触发建立 IPSEC VPN 隧道的条件,LAN-to-LAN 的 VPN 隧道建立,两个校区可以通过广域网链路继续通信。

(3)当裸光纤链路恢复后,OSPF 的路由优先级比浮动静态路由高,因此数据会再次切换回两个校区之间的核心交换机转发。

由于采用了 IPSEC 加密,因此即使传输在公网上 VPN 隧道内的两个校区之间通信数据也不会被恶意截获、也无法被轻易破解。SVN 支持多种加密算法(3DES\DES、RC4、AES 及 RSA)和 Hash 算法(包括 MD5、SHA-1),确保了数据传输的真实性、完整性。

3 建设的成效

(1)选用高性能防火墙,满足了师生高流量、高并发外网访问需求。

校园网出口采用华为公司的统一安全网关,如 USG5300 系列。该网关采用先进的多核硬件架构,多线程并行处理,优化了安全业务处理流程,特别是针对首包处理的优化,使 USG5300 系列统一安全网关具备同档产品业界第一的每秒新建连接数,足以应对各种大规模网络流量的应用。同时,将数据解封装和深度检测进行分离,实现多种深度检测并行,大幅度提升设备在深度检测状态下的性能。多年来成功的商业应用,成熟的 VRP[10]软件平台为 USG5300 系列统一安全网关提供健壮的操作系统,是用户最可信赖的安全操作系统。

(2)利用超强 DDoS 防护功能,提供了校园网出口绿色防护。

对关键网络业务的 DDoS 防护,是学校师生面临的重大安全问题之一。华为 USG5300 系列统一安全网关凭借超高的每秒新建连接数,对于 DDoS 攻击的防护可以达到每秒数百万包以上,为用户的业务系统提供 DDoS 攻击防护、强大的协议分析能力,可有效支持对 SYN FLOOD、UDP FLOOD、ICMP FLOOD、DNS FLOOD、CC[11]等多种 DDoS 攻击种类的准确识别和控制,还能提供蠕虫病毒流量的识别和防范能力,结合华为公司专有 ICA[12]智能连接算法,保证在准确识别 DDoS 攻击流量的同时,不影响用户的正常访问,有效提供校园网异常流量清洗、防护。

(3)采用 P2P 防护,提升了师生互联网访问感受。

P2P 流量已成为校园网目前最大的困扰,严重时会导致学校内的业务应用无法正常进行。由于 P2P 协议具有的灵活特性,使得对其控制成为一个难题。采用统一安全网关是基于强大的网络协议分析能力,可以实现对几十种 P2P 流量的精确识别,同时,可支持特征库升级,不断识别新的协议种类,对各类 P2P 协议实现 K 级流量控制,有效地保障用户的网络带宽资源,帮助学校合理规划网络流量,提升校园网络应用价值,有效提升全校师生的上网感受。

(4)实现 UTM 统一安全管理,满足了师生高流量、高并发外网访问需求。

系统采用 IPS 入侵检测引擎功能,配合先进的软、硬件平台及丰富的签名库,通过统一安全网关能够快速、精确识别出混杂在正常流量中的应用层攻击,实时捕获最新的攻击、蠕虫、木马等威胁[13],提取相应签名,并能及时为统一安全网关提供更新,从而保证了 UTM 的防御能力,为校园网出口提供 5-7 层的安全防护,满足了师生高流量、高并发外网的访问需求。

4　结束语

对于多校区数字校园网络建设时,抓住建设机遇,在校园网络安全建设工作过程中,按区域、分层次构筑了校园网安全体系架构,实现了整体的立体安全防护效果。图 6 概括了高校校园网安全建设的总体效果。

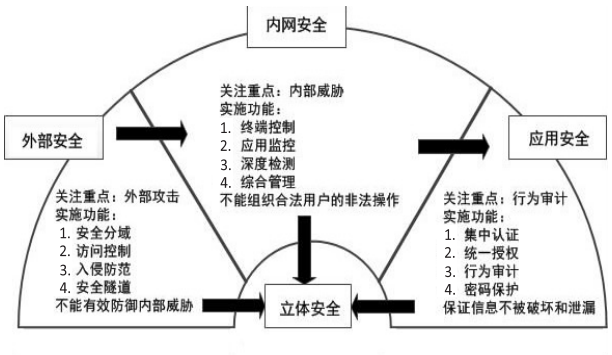

图 6　校园网安全建设效果图展示

通过校园网安全建设,有效保障了学校的信息网络安全,使校园网的安全建设水平达到了新的高度,同时对同类高校的校园安全建设有较大的指导意义。

参考文献:

[1] 王智贤. 基于数字校园建设的校园网安全解决方案[J]. 计算机安全,2010(11):93-94.

[2] Nguyen H V, Choi Y. Proactive detection of DDoS attacks utilizing k-NN classifier in an anti-DDos framework[J]. International Journal of Electrical, Computer, and Systems Engineering, 2010, 4(4): 247-252.

[3] Zhang Xingang. Analysis of new security issues in the development of higher education informatization[C]//Proceedings of 2010 international conference on information, electronic and computer science. [s. l.]: Scientific Research Publishing, 2010: 1967-1971.

[4] 傅　川,陈　云. 高校信息系统安全体系研究与实践[J]. 中山大学学报:自然科学版,2009,48(S):25-28.

[5] Wang Baoping. Available separation-of-duty policies in access control[C]//Proceedings of 2010 international conference on networks security, wireless communications and trusted computing. [s. l.]: IEEE Computer Society, 2010: 290-293.

[6] 刘　刚,张　宏,李千目. 基于博弈模型的网络安全最优攻防决策方法[J]. 南京理工大学学报:自然科学版,2014,38(1):12-21.

[7] 张　瑞. 北京师范大学构筑校园网防毒围城[J]. 中国教育网络,2010(6):47-48.

[8] 闻德军,张代远. 计算机网络安全与防护技术研究[J]. 计算机技术与发展,2012,22(12):171-174.

[9] 张新刚,张鸿军. 网络教育环境下的新型安全威胁分析及其防范[J]. 中国电化教育,2007(11):110-112.

[10] 黄　瑞,邹　霞,黄　艳. 高校信息化建设进程中信息安全问题成因及对策探析[J]. 现代教育技术,2014,24(3):57-63.

[11] Zhang Xingang. Analysis of campus network security emergency response linkage system[C]//Proceedings of 2010 international conference on information technology and industrial engineering. [s. l.]: World Academic Press, 2010: 1016-1020.

[12] 周永帅,张　毅,吴　凯. 多校区校园网络身份认证系统的现状与发展[J]. 中国医学教育技术,2014,28(1):41-45.

[13] 丁　健. 浅谈网络安全技术与管理[J]. 计算机安全,2013(12):64-66.

数字校园网络立体化安全防护的研究

作者： 蒋建军， JIANG Jian-jun
作者单位： 上海电机学院 网络信息中心，上海 200240; 武汉理工大学 信息工程学院，湖北 武汉 430070

刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2015(9)