

# 中小企业内网安全管理的研究与实现

甘 丽<sup>1</sup>, 胡 昊<sup>2,3</sup>

(1. 安徽工业大学 工商学院, 安徽 马鞍山 243002; 2. 东南大学, 江苏 南京 210096;  
3. 马钢自动化工程公司, 安徽 马鞍山 243002)

**摘 要:**随着信息技术的发展以及企业管理的需要,大多数企业建立了自己的内网。但由于计算机终端的数量众多、企业内部网络安全管理的落后,导致企业内网也常常面临危险的困境。文中通过对“基于端口的网络接入控制”这一技术的研究,对接入网络的端口加以控制,实现用户级的接入控制,并对每种不同类型的用户给予不同的权限,从而实现对整个网络安全的管理。以给某设计院设计内网安全管理为例,对其设计的方法进行分析和描述。通过系统的实际运行表明:该方法在保障企业内网安全问题上有明显的效果。

**关键词:**企业内网;安全管理;基于端口的网络接入控制

**中图分类号:**TP309

**文献标识码:**A

**文章编号:**1673-629X(2013)08-0122-03

doi:10.3969/j.issn.1673-629X.2013.08.031

## Research and Implementation of SME Network Security Management

GAN Li<sup>1</sup>, HU Hao<sup>2,3</sup>

(1. Industrial & Commercial College, Anhui University of Technology, Ma' anshan 243002, China;  
2. Southeast University, Nanjing 210096, China;  
3. Masteel Control Technology Co., Ltd., Ma' anshan 243002, China)

**Abstract:** With the development of information technology, as well as the needs of the enterprise management, the majority of enterprises have established their own internal network. However, due to the large number of computer terminals, the backwardness of internal network security management, enterprise network often face dangerous predicament. Through study of "Port-based network access control" technology, control the access network port to achieve user-level access control, and give different permissions to each of the different types of users, thereby the management of the entire network security. Take design of internal network security management to a design institute for example, the design method is analysed and described. Through the actual operation of the system, the method had a significant effect on the issue of the protection of the security of the enterprise network.

**Key words:** enterprise network; security management; port-based network access control

## 0 引 言

信息系统是现代企业不可缺少的重要技术设施,计算机则已经成为了不可或缺的办公及生产工具。数量众多、应用广泛的计算机终端的维护和管理对于众多企业都是一件难事。一方面,由于计算机病毒、木马和蠕虫的不断出现、攻击事件时有发生,终端系统必须经常升级和更新配置,才能增强对这些安全威胁的抵抗。但终端使用者在计算机操作方面的专业素养参差不齐,再加上个人的安全知识、安全意识以及个人习惯的不同,往往难以独立保证终端系统的安全运行。另一方面,企业制订出符合业务安全标准的安全策略需

要有比较丰富的安全管理实践和深厚的安全技术基础。即使企业制订出了完善的安全策略,但是如果没有合适的技术工具的配合,就难以保证每个终端都会快速准确地按照企业制订的策略进行安全部署,IT管理人员也难以实时跟踪实施情况,导致安全策略难以有效执行下去,安全策略成为一纸空文。

一些传统的认证方式也可以达到一定的效果,但其存在的弊端制约了其在内部网络的发展。如传统的PPPoE认证系统,认证过程需要把每个网络包拆解,才能识别和判断用户的合法性。大量的拆包解包过程必然需要硬件配置较高的宽带接入服务器来完成,伴随

收稿日期:2012-09-09

修回日期:2012-12-11

网络出版时间:2013-04-08

基金项目:马钢集团设计研究院网络安全管理系统工程项目(KQ0912-010DB)

作者简介:甘 丽(1985-),女,安徽马鞍山人,硕士,研究方向为信息管理。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20130408.1631.043.html>

而来的是网络建设成本的上升。接入服务器拆封并转发每个用户的数据包,一旦用户并发增多,还会造成网络访问的瓶颈<sup>[1]</sup>。其他认证方式,如 Web/Portal 认证方式,虽然不需要特定的客户端软件,部署方便,同时可提供 Portal 等增值业务。但缺点是其协议承载于应用层,一般采用出口网关设备,对内部网络来说,存在安全隐患,如论坛中的过激言论或是 IP 攻击服务器等行为都无法追踪源<sup>[2]</sup>。而基于端口的访问控制协议认证,即 802.1X 认证方式,在局域网接入设备的端口这一级对所接入的接入设备进行认证和控制。802.1X 协议为二层协议,对设备的整体性能要求不高,可以有效降低网络建设成本,采用“可控端口”和“不可控端口”的逻辑功能,从而可以实现业务流与认证流分离,有利于解决网络瓶颈<sup>[3]</sup>。

1 802.1X 协议

802.1X 协议是一种基于端口的网络接入控制协议。“基于端口的网络接入控制”指的是对接入内网的计算机、工程师站等网络设备,在接入设备端口这一级进行网络认证和控制。连接在接入设备端口上的用户设备如果能通过网络安全认证,就可以访问网络;反之若不能通过认证,则无法接入网络,访问网络资源<sup>[4]</sup>。

1.1 802.1X 的体系结构

使用 802.1X 的系统,为典型的 C/S 体系架构,如图 1 所示分别为: Supplicant System(客户端系统)、Authenticator System(认证设备系统)以及 Authentication Server System(认证服务系统)<sup>[5]</sup>。

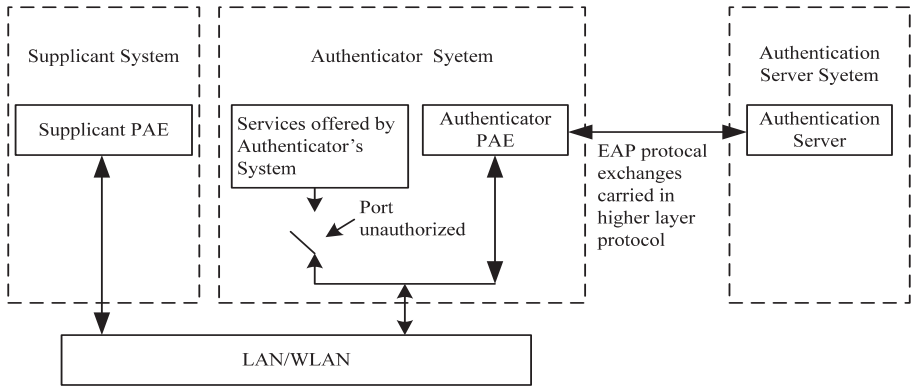


图 1 802.1X 认证系统的体系结构

(1)客户端系统是位于内部网络的一个实体,当其需要接入网络时,由位于该内部网络的认证设备系统对其进行接入认证。客户端系统一般为用户终端设备,用户需要在其终端上安装支持 EAPOL( Extensible Authentication Protocol Over LAN,基于局域网的扩展认证协议)协议的软件,进行 802.1X 认证。

(2)认证设备系统是用于对所连接的客户端系统

安全认证的另一实体,也位于内部网络。认证设备系统为客户端系统提供内网认证接入端口,可以是逻辑端口,也可以是物理端口,认证设备系统一般为支持 802.1X 协议的网络设备。

(3)认证服务器系统是为认证设备系统提供认证服务的实体,认证服务器系统一般为 RADIUS<sup>[6]</sup> ( Remote Authentication Dial-In User Service,远程认证拨号用户服务)服务器,用于实现接入网络用户的认证、授权和计费,认证服务器存储了用户接入网络的关键信息,一般包含用户的上网账号、上网密码、接入用户所在的虚拟局域网、服务优先级、访问控制列表等信息。

1.2 802.1X 的工作机制

802.1X 认证系统在客户端系统和认证服务器系统之间交换认证信息,主要用到 EAP( Extensible Authentication Protocol,扩展认证协议)协议<sup>[7]</sup>。在客户端系统 PAE( Port Access Entity,端口访问实体)与认证设备系统端口访问实体之间,如果是局域网环境,则扩展认证协议报文使用基于局域网的 EAPOL 封装格式,直接承载于局域网环境当中<sup>[8]</sup>。

图 2 为 802.1X 认证系统的工作机制。

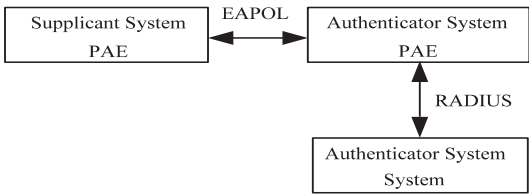


图 2 802.1X 认证系统的工作机制

(1)在认证设备系统端口访问实体与 RADIUS 服务器之间,扩展认证协议报文既可以使用 EAPOR<sup>[9]</sup> ( EAP Over RADIUS, 基于 RADIUS 的扩展认证协议)封装格式,承载于 RADIUS 协议中;也可以由设备端口访问实体终结,转而在设备端口访问实体与 RADIUS 服务器之间传送其它协议,如 PAP<sup>[10]</sup> 协议报文或 CHAP<sup>[11]</sup> 协议报文。

(2)当用户发送认证消息后,接收来自认证服务器的消息,同时接收用户网络权限相关信息,认证设备系统端口访问实体根据 RADIUS 服务器通过或未通过指示,控制端口的授权状态。用户可接入网络,说明已经通过网络安全认证,端口由非授权转变为授权状态;用户无法接入网络,则会有返回信息提示没有通过认证,这时受控端口状态不变,仍然为非授权状态<sup>[12]</sup>。

## 2 应用实例

某设计院设有 8 个职能管理部门,8 个工程设计研究所和 1 个工程咨询分公司,设计院原有网络设计为内网终端通过代理服务器对 IP 地址进行认证,认证通过后授权接入 Internet,这样的网络设计只能控制终端能否访问 Internet,无法对控制终端能否接入内部网络。外来用户只要知道 IP 地址,就可以随意接入内部网络,造成内部机密文件外泄。

### 2.1 需求分析

针对存在的安全问题,该设计院对新的网络建设提出了以下几点需求:

- (1) 方便易用,部署灵活,配置简单;
- (2) 能对终端接入控制功能,不同用户不同权限,保障企业内网安全;
- (3) 能够对终端用户身份合法性认证检查,阻断非法用户访问内部网络;
- (4) 能够检查终端的安全性,隔离并修复不安全终端,保障内部网络免受病毒侵害;
- (5) 能够对内部制定的安全策略强制执行,加强信息安全管理;
- (6) 能对用户行为监控和审计,防止信息泄密;
- (7) 能对交换机、路由器、防火墙等网络设备进行统一管理。

### 2.2 网络拓扑

针对该设计研究院的以上需求,以优化网络结构,提升网络性能为目的,设计网络拓扑结构如图 3 所示。

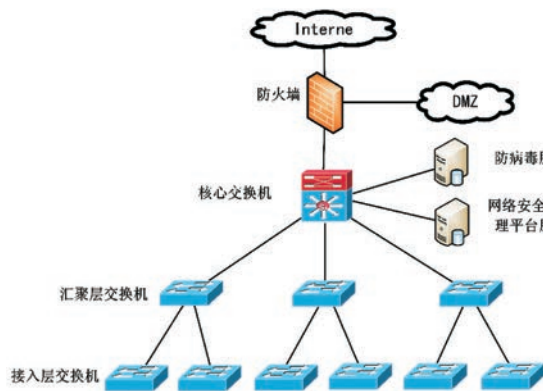


图 3 整体网络拓扑结构

整体采用星型拓扑结构,以办公楼五楼机房为网络中心,配置核心交换机 1 台,汇聚交换机 3 台,每层楼配置接入交换机 2 台。两台服务器直接接入核心交换机,分别是防病毒管理服务器和网络智能管理平台服务器,网络智能管理平台服务器主要作用是用户的接入认证管理。防火墙配置 DMZ 区域放置 Web 服务器提供对外网的 Web 访问服务。

### 2.3 终端安全系统的部署

终端安全系统对接入内部网络用户的终端设备,

实施安全检查后的网络准入策略,通过安装在用户终端上的客户端软件、服务器端的安全策略组件、网络层面的网络接入设备以及和第三方软件的互动,多方面入手,严格控制用户使用的网络的权限,从而达到加强用户终端主动防御能力,保护内部网络安全的目的。

系统包含两台服务器,分别安装智能管理中心服务器和防病毒服务器,用户终端强制安装 802.1X 安全客户端。对接入交换机配置 802.1X 认证协议,配合智能管理中心服务器完成联动,完成身份认证后,由服务器根据不同用户权限动态下发访问控制列表。

智能管理中心服务器在用户终端通过检查最新病毒库、检查最新漏洞补丁等安全扫描后,根据用户角色拥有的不同网络访问权限定义不同的安全策略,将对应的网络访问控制列表下发给网络接入设备,按照角色权限规范用户的网络使用行为,严格控制网络接入。用户的所属虚拟局域网、访问控制列表等安全措施均可由网络管理员在服务器上操作,即使底层接入设备不支持 802.1X 协议,只要上层设备支持,也能做到根据不同的用户执行不同的控制。

## 3 结束语

随着企业管理的深入,特别是企业内部网络管理的深入,内网的安全性已经是一个刻不容缓的问题。802.1X 认证协议可以比较好地解决现阶段的企业内部网络所面临的身份认证和应用终端的安全性问题。但要深刻地理解到要构建一个真正的安全可靠的网络环境仅仅依靠 802.1X 这一项技术是不够的,只有将技术与管理相结合才能从根本上解决问题。

### 参考文献:

- [1] 刘梅. 基于 802.1X 的校园网接入认证安全防御[J]. 中国教育网络, 2012(2): 54-56.
- [2] 刘小飞. 多种宽带接入认证方式[J]. 产业与科技论坛, 2011(7): 134-135.
- [3] 罗汉云, 宋勇. 802.1X 认证技术分析[J]. 安庆师范学院学报: 自然科学版, 2009, 15(1): 52-54.
- [4] 谢希仁. 计算机网络[M]. 北京: 电子工业出版社, 2008.
- [5] 华为 802.1X 技术白皮书[M]. 出版地不详: 华为技术有限公司, 2001.
- [6] Rigner C, Willens S, Rubens A, et al. Remote Authentication Dial in User Service (RADIUS)[S]. RFC 2865, 2000.
- [7] IEEE Standard for Local and Metropolitan Area Networks—Port-based Network Access Control[S]. IEEE 802.1X 2010, 2010.
- [8] Extensible Authentication Protocol (EAP)[S]. RFC 3748, 2004.



策略路由是数据包转发规则,依据用户制定的策略进行路由选择的机制,与单纯依照 IP 报文的目的地址查找路由表进行转发不同,可应用于安全、负载分担等目的<sup>[8]</sup>。路由器中存在两种类型和层次的表,分别是路由表和转发表。转发表是由路由表映射过来的,策略路由直接作用于转发表,不改变路由表中任何内容。

路由策略是路由发现规则,在正常的路由协议之上,根据某种规则,通过改变某些参数或者设置某种控制方式来改变路由产生、发布、选择的结果,最终改变的是结果(即路由表)。路由策略直接作用于路由表,是在路由发现的时候产生作用。

策略路由的优先级高于路由策略,当路由器进行数据包转发的时候,会优先匹配策略路由的规则,如果匹配一致,则按照策略路由来转发,否则根据路由表中的转发路径来转发<sup>[9]</sup>。

## 4 策略路由在多出口校园网中的应用

我国高校信息化建设正在经历巨大变迁,数字校园的建设包括三个层面:基础网络设施;公共服务体系,如邮件服务、安全防护等;业务应用层包括教学应用、科研应用、管理应用等。校园网单一接入教育网模式已不能满足广大师生的网络需求。许多高校增加了教育网以外的其他 ISP 连接,比如电信、联通等,形成了多出口校园网络结构。

为了保证网络的可用性,国内许多高校采用同时接入教育网和电信(或联通、移动)等多网接入方案,实现多链路并行<sup>[10]</sup>。由于教育网和公众网不同网络运营商之间的网络连通性问题,校园网用户访问不同的 ISP 时速度明显变慢。校园网的路由有特殊需求,多出口网络结构使得路由实现及相关问题更加复杂。

对于校园网,需要根据源 IP 地址进行路由选择,强制其通过指定出口进行路由转发,访问教育网资源走教育网出口,访问其他资源走公网出口。这样,一方面提高了出口速度,另一方面也提高校园网出口的冗余,增加校园网的稳定性<sup>[11]</sup>。在电信、联通出口实现 NAT,禁止校园网用户从教育网出口访问收费站点资源,有效减少教育网的国际流量费用。针对需要访问教育网资源的校园网用户制定源地址路由,这样不仅

降低网络运行费用,还能防止校园网一个链路发生故障而断开和 Internet 的连接<sup>[12]</sup>。文中提出的策略路由和 NAT 相结合的配置方案,能够充分利用现有网络的多出口,尽可能地节约校园网运行成本,为广大师生提供可靠高效的网络访问。

## 5 结束语

策略路由和 NAT 相结合的方案,可以应用于多出口校园网络环境中,使校园网用户能通过不同的出口访问教育网、电信、联通等不同的网络资源。在出口防火墙应用策略路由,可以合理使用网络有限出口的宽带资源,实现网络负载均衡,提高资源利用率,保障校园网安全。

### 参考文献:

- [1] Cheswick W R, Bellovin S M, Rubin A D. Firewalls and internet security: repelling the wily hacker[M]. Beijing: China Machine Press, 2003.
- [2] Al-Tawil K, Al-Kaltham I A. Evaluation and testing of Internet firewalls[J]. International Journal of Network Management, 2002, 9(3): 135-149.
- [3] 谈 华. 硬件防火墙在网络安全中的应用[J]. 电脑知识与技术: 学术交流, 2007(19): 73-74.
- [4] 田 原, 云晓春, 朱晓辉. 防火墙性能基准测试研究[J]. 计算机仿真, 2003, 20(7): 123-125.
- [5] 陈志平. 校园网络安全与防火墙技术[J]. 现代计算机, 2007, 25(1): 47-49.
- [6] 刘建伟, 张卫东. 网络安全实验教程[M]. 北京: 清华大学出版社, 2007.
- [7] 贾学锋, 荆一楠, 王雪平, 等. 基于 TCP 协议的 NAT 穿透技术在 P2P 中的研究与实现[J]. 计算机应用与软件, 2008, 25(6): 186-187.
- [8] 张焕杰, 孟庆宇, 杨寿保. 基于 Linux 系统的校园网多出口策略路由实现[J]. 通信学报, 2006(21): 130-133.
- [9] 翟 钰, 武舒凡, 胡建武. 防火墙包过滤技术发展研究[J]. 计算机应用研究, 2004(9): 144-145.
- [10] 张红梅. 策略路由在校园网中的应用[J]. 宁波工程学院学报, 2005, 17(4): 28-30.
- [11] 姚亚锋, 方贤进, 赛文莉. 新型内容过滤防火墙的研究[J]. 计算机技术与发展, 2010, 20(11): 158-161.
- [12] Verma D. Simplifying Network Administration Using Policy Based Management[J]. IEEE Network, 2002, 16(2): 20-26.
- [9] Rosenberg J, Weinberger J, Huitema C, et al. STUN-Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators(NATs)[S]. IETF RFC 3489, 2003.
- [10] 秦 刘, 智英建, 贺 磊, 等. 802.1X 协议研究及其安全性分析[J]. 计算机工程, 2007, 33(7): 153-154.
- [11] 凤 琦, 王震宇, 李向东, 等. 基于 802.1X 的可信网络连接技术[J]. 计算机工程, 2009, 35(5): 165-167.
- [12] 刘海韬, 张 浩. 结合 802.1x 技术实现网络安全管理[J]. 计算机技术与发展, 2009, 19(7): 170-172.

(上接第 124 页)

# 中小企业内网安全管理的研究与实现

作者：[甘丽](#)，[胡昊](#)，[GAN Li](#)，[HU Hao](#)

作者单位：[甘丽, GAN Li \(安徽工业大学 工商学院, 安徽 马鞍山, 243002\)](#)，[胡昊, HU Hao \(东南大学, 江苏 南京 210096; 马钢自动化工程公司, 安徽 马鞍山 243002\)](#)

刊名：[计算机技术与发展](#)

ISTIC

英文刊名：[Computer Technology and Development](#)

年，卷(期)：2013 (8)

本文链接：[http://d.wanfangdata.com.cn/Periodical\\_wjfz201308031.aspx](http://d.wanfangdata.com.cn/Periodical_wjfz201308031.aspx)