doi:10.16055/j.issn.1672-058X.2015.0007.021

基于 VPN 技术的数据中心系统管理模式和安全策略设计*

门 华
(重庆工商大学 信息化办公室,重庆 400067)

摘 要:传统的数据中心系统管理安全模式存在高风险的安全隐患,而 VPN 是一种建立在开放的 Internet 并适合于系统管理的安全技术.通过对传统数据中心系统管理方式的问题分析,提出了基于 VPN 技术的系统管理模式,并以此设计出基于角色的安全策略,解决了传统管理模式安全性问题,通过在重庆工商大学数据中心的部署和实施,验证了该模式的系统管理安全性.

关键词: VPN;数据中心;系统管理;安全策略;角色
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1672-058X(2015)07-0091-05

随着信息化的不断发展,各类管理系统及数据急剧增加,数据中心实现了全面、集中、有效的管理,保障了各项业务的顺利运行和服务的及时提供.近年来,云平台和虚拟化技术加入,使得数据中心朝着集成化和专业化的方向快速发展,随之带来的网络安全问题也日益突出,成为亟待解决的热点问题。数据中心一般提供两类人群的访问:普通用户,访问数据中心提供的通用服务和资源;系统管理员,负责进行相关的信息系统日常管理和软硬件维护.通常情况下,数据中心的安全防护主要针对普通用户的访问方式,然而,系统管理员拥有比普通用户更多的访问权限,因此其访问方式的安全性更值得关注和研究.

传统的数据中心系统管理方式存在以下问题:使用显示器、键盘或者 KVM 系统进行管理的方式,系统管理员必须进入机房在服务器硬件上进行操作,安全性高但缺乏便捷性,网络服务具有 24 小时不间断的特点,要求管理员 365 天 24 小时及时响应,这种方式往往难以达到;单纯使用 telnet、远程桌面、ssh 等管理方式,虽然解决了远程管理的问题,但个别管理方式如 telnet 甚至没有使用加密技术,安全性极低,其他使用了加密技术的管理方式,安全性只能依赖管理软件自身,也存在着很大的安全隐患[1],无法对系统管理员进行统一管理和审计[2],只能针对每一台服务器进行用户权限的分配和审核,不能进行整个数据中心系统管理权限的规划和全局设计,导致权限管理混乱.

针对以上问题,提出一种基于 VPN 的数据中心系统管理模式,并在此基础上进行基于角色的安全策略设计.VPN 能够利用加密通讯协议在公共网络中建立安全可靠的数据传输通道, 通过对 VPN 进行合理的架设,有效规避系统管理员远程管理时带来的安全问题,同时设计更合理的安全策略,降低安全风险[3].

收稿日期:2014-12-13;**修回日期**:2015-01-20.
* **基金项目**:重庆市教委科学技术研究项目资助(KJ1400643);重庆工商大学教改研究重点项目资助(2014220).
作者简介:门华(1977-),男,四川内江人,硕士,高级工程师,从事计算机网络研究.

1 VPN 技术

VPN 又名虚拟专用网络,是一种在开放的、不安全的 internet 上,建立安全的数据通道,将每一个用户的通信分离开传输的技术[4].VPN 采用复杂的算法,结合认证技术、隧道技术、加密技术和网络技术传输数据,使得数据不被窃取和篡改,保证数据的真实性.VPN 通道从 VPN 设备或 VPN 终端开始,横跨 internet,到达其他 VPN 设备,非常适合系统管理远程访问的需要和安全性的要求[5].

当前主流的 VPN 技术有 L2TP/IPSEC VPN,SSLVPN 等,各种 VPN 的工作原理类似,以 SSLVPN 为例,它的工作原理如图 1 所示.

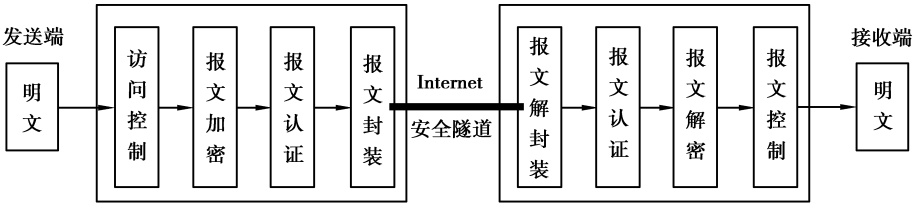

图 1 SSL VPN 的工作原理

VPN 是在 Internet 的两端通过访问控制、报文加解密、报文认证、报文封装及解封装等技术建立起一条安全隧道,使得传输的数据不被窃听、篡改,保证报文的完整性和机密性.

2 系统管理模式的建立和安全策略设计

与普通用户不同,系统管理员拥有配置后台、管理数据库、管理操作系统等高级权限,因此对他进行系统操作的管控必须更加严格.研究提出一种基于 VPN 的系统管理模式,并在此基础上设计基于角色的安全策略,来加强系统管理的控制能力,降低安全风险.

2.1 基于 VPN 的系统管理模式的建立

合理搭建 VPN 设备是基于 VPN 的系统管理模式的关键,首先在数据中心出口部署一台防火墙设备,使系统管理员从内网到外网都不允许直接对服务器进行管理;其次在防火墙内侧搭建 VPN 设备,允许系统管理员通过 VPN 进行管理.

通过合理架设 VPN 实现对数据中心系统管理的三重安全防范:①防火墙过滤及防护[7].将 VPN 设备架设在数据中心防火墙内侧,可以发挥防火墙的安全防范优势,第一层过滤 ddos,flood 洪泛等攻击,进行包过滤、内容过滤、访问控制等安全防范;②数据流的封装和加密.系统管理员在终端到 VPN 设备之间建立隧道,将传输的数据流进行封装和加密,防止数据被篡改和窃取;③身份认证和权限分配.通过身份认证和权限分配,只有合法的系统管理员身份才能获得相应的系统访问权限,访问相应的资源.

系统管理员需通过防火墙和 VPN 共同实现的三重安全防范后,才能对数据中心的相应服务器进行系统管理,系统管理员访问路径如图 2 所示.基于 VPN 的系统管理模式解决了系统管理的远程管理和安全性问题.

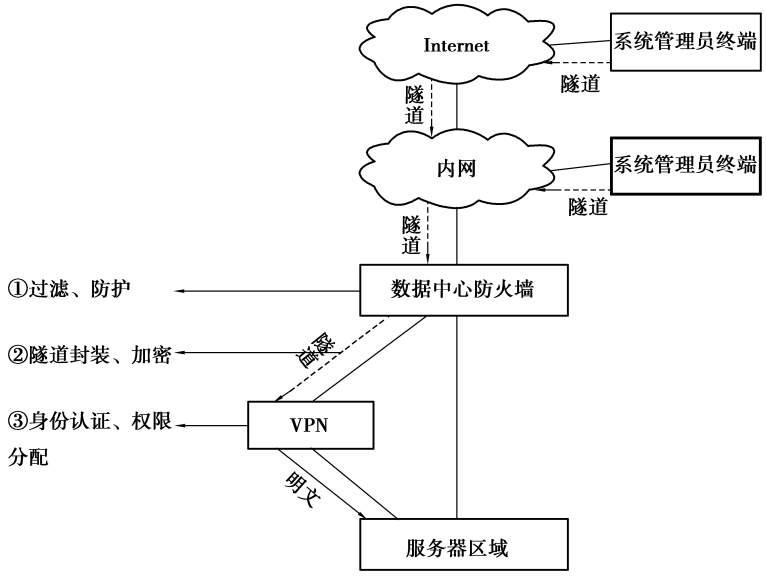

图 2　系统管理员访问路径图

2.2　基于角色的安全策略设计

VPN 技术是系统管理安全性的前提,在此基础之上,制定相应的安全认证策略是保障系统管理安全的关键.数据中心通常拥有众多服务器区域,包括数据库服务器区、核心应用服务器区、普通应用服务器区、托管区等.每个区域的管理权限分为多个级别,如硬件资源级、操作系统级、应用系统级等,不同级别又能够继续细分.权限的划分庞大而复杂,因此以科学合理的方式管理和使用这些权限成为系统安全策略的重点.基于角色的访问控制是安全策略中一种有效的权限管理方式,研究采用基于角色的访问控制作为安全策略的基本方法.

基于角色的访问控制(Role-Base Access Control,简称 RBAC)主要由用户、角色和权限 3 个实体组成.角色根据组织内工作性质的不同来设定,用户根据所担负的责任被赋予某种角色.用户可以通过赋予不同的角色而拥有不同的权限. 如果有新的功能加入,角色相应地就被赋予新的权限. 角色的权限既能被赋予也能被撤销.权限和角色是多对多的关系,角色和用户也是多对多的关系,用户跟权限之间没有直接的关系.

在基于 VPN 的数据中心系统管理安全策略中,用户指系统管理员,分为组织外和组织内.组织外的系统管理员为厂商、集成商及技术服务商等技术人员,组织内的系统管理员为数据中心技术管理人员,其他部门的系统后台管理人员等.角色指具有某些共性的系统管理员组成的集合,包括超级管理员、应用软件管理员、网站管理员等.权限指规定了的一系列数据中心服务器访问规则,具体表示为服务器 ip 地址+端口的访问权限.

数据中心系统管理安全策略的具体设计:

权限设计.权限根据服务器(包括虚拟服务器)提供的服务进行设计,每一种权限的基本元素是服务器 ip 地址、开放端口、动作(允许或拒绝).对每一台服务器提供的所有服务进行权限的细分.

角色分级.第一级为超级管理员,可以管理所有区域的服务器;第二级为区域管理员,按照数据中心区域来划分,可以管理本区域的服务器,如数据库区管理员;第三级为应用系统管理员,按照应用关系来划分,如教务系统管理员,他可以管理教务系统数据库、应用服务器等;第四级为应用系统操作员,只需对应用系统后台进行管理,如网站后台管理员等.

用户定义.一个系统管理员,可能身兼多职,既要负责教务系统的管理,也要负责教务处网站的管理,就要对这个用户定义多个角色.

系统管理员使用终端首先连接到VPN上建立隧道,通过隧道进行数据的加密传输,然后在VPN上进行用户认证,合法用户认证成功后,获取已经定义好的角色,再根据角色加载已配置好的权限,就可以进行相应的系统管理操作.

基于角色的安全策略解决了系统管理的统一设计、统一管理的问题.

3 重庆工商大学数字中心平台的部署实施

3.1 实施环境

重庆工商大学数据中心现有服务器、存储器100余台,分为统一存储区、核心应用区、普通应用区、托管区、专网区,提供数字校园的各种应用服务.数据中心出口架设阿姆瑞特防火墙AS-F5500一台,该防火墙集成VPN功能.

3.2 部署概述

为验证本研究的安全合理性,有效解决重庆工商大学数据中心系统管理的安全性问题,现将VPN及本研究的安全策略部署于防火墙上,并开启防火墙的访问控制功能,不允许系统管理员直接访问服务器,只能通过VPN来访问.为解决系统管理员外网连接内网VPN问题,对VPN的拨入私有地址做外网公有地址映射,并做内外网统一域名解析,方便系统管理员连接VPN.系统管理员在终端进行相应配置,连接VPN统一域名,认证成功后就可得到对应权限访问相应服务器.重庆工商大学数据中心拓扑结构图如图3所示.

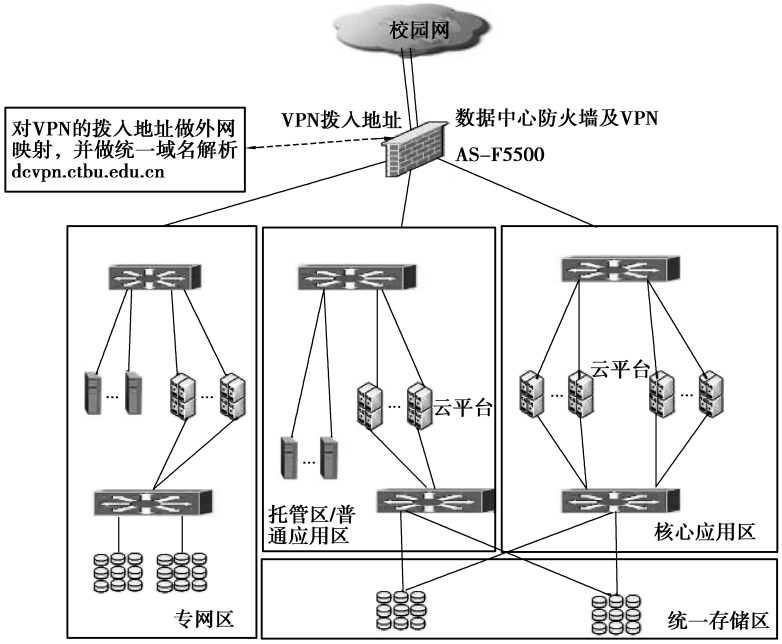

图3 重庆工商大学数据中心拓扑结构图

3.3 运行结果

基于VPN技术的系统管理模式和安全策略在重庆工商大学数据中心成功部署,经过几个月的试运行,取得了良好的效果.成果如下:实现内外网无差别管理和远程管理.无论是在校园网内网或外网,都拨同样的VPN域名,系统管理员在逻辑上无差别.安全性更高.首先系统管理员不能直接访问服务器进行管理,其次通过VPN的数据都进行了封装和加密,保证了其安全性.统一的管理日志.VPN设备会记录所有系统管理员的连接日志,便于管理和事件记录跟踪.统一的权限设计和细粒度的权限管理.建立了全局的基于角色的安全

策略,对权限的管理更加细致和严格.

4　结束语

数据中心的管理者已经逐渐意识到系统管理安全的重要性,基于 VPN 技术的系统管理模式能够提高传统系统管理的安全性,而在此基础上设计出来的基于角色的安全策略,能够更加严格、细致地进行权限划分和规范,避免权限划分过粗导致的权限安全问题.VPN 生成的统一日志管理允许快速查找、跟踪系统管理员的操作情况,便于故障排查,问题回溯.因此,有效地避免了系统管理员远程管理时带来的安全问题,保障了网络安全性.随着数据中心的应用不断增多,相关权限也在不断变化,基于角色的安全策略也需不断地修改以适应新的系统管理需求.

参考文献:

[1] 应国良,田京波.基于 SSL VPN 的核心机房远程管理系统的设计与实现[J].网络教育与远程教育,2007(8):39-42

[2] 刘胜国,徐志根,刘雁林,等.基于审计与访问控制的授权策略研究[J].计算机工程与设计,2006,27(22):4268-4270

[3] SINGH A K, SAMADDAR S G, MISRA A K. Enhancing VPN Security Through Security Policy Management[C]//International Conference on Recent Advances in Information Technology. 2012

[4] 魏广科.VPN 技术及其应用的研究[J].计算机工程与设计,2005,26(3):714-715;724

[5] 秦鸿.利用 VPN 技术实现远程访问的研究与实践[J].图书情报工作,2007,51(3):117-120

[6] CH F,WU K H, CH W, et al.The Research and Implementation of the VPN Gateway Based on SSL[J].Computational and Information Sciences (ICCIS), 2013,364:1376-1379

[7] 宿洁,袁军鹏.防火墙技术及其进展[J].计算机工程及应用, 2004(9):147-149;160

System Management Mode and Security Policy Design of Datacenter Based on VPN

MEN Hua

(Network Information Office, Chongqing Technology and Business University, ChongQing 400067,China)

Abstract: There is high risk of potential safety hazard for traditional system management mode of datacenter, and VPN is a kind of security technology based on open internet and suitable for system management. By the analysis of traditional datacenter management system, this paper puts forward system management based on VPN technology and designs the role-based security policy, which solves the security problems of the traditional management mode. The system management mode is verified secure by the deployment and implementation of Chongqing Technology and Business University datacenter.

Key words: VPN; data center; system management; security policy; role