文章编号：2095-4980(2019)01-0158-04

中小型企业网络安全方案的设计

屈正庚[1]，吕　鹏[2]

(1.商洛学院 数学与计算机应用学院，陕西 商洛 726000；2.西安理工大学 计算机科学与工程学院，陕西 西安 710048)

摘　要：为了提高企业竞争力和经济效益，以中小型企业为例，分析了网络安全的相关理论技术，探讨了中小型企业网络安全需求，理清现有中小型企业整个网络结构和网络拓扑图，对其存在的问题进行了梳理，然后设计了一个较为完善的企业网络拓扑图。从物理环境安全、网络边界安全、网络内部安全等方面进行了加固和规划，提高中小型企业的网络安全等级。

关键词：网络安全；防火墙；拓扑图；设计方案

中图分类号：TN926　　**文献标志码：**A　　**doi：**10.11805/TKYDA201901.0158

Network security scheme design for small and medium-sized enterprises

QU Zhenggeng[1], LYU Peng[2]

(1.School of Mathematics and Computer Application, Shangluo University, Shangluo Shaanxi 726000, China;
2.School of Computer Science and Engineering, Xi'an University of Technology, Xi'an Shaanxi 710048, China)

Abstract: In order to improve the competitiveness and economic benefits of enterprises, the use of network technology for business processing is the inevitable trend of social development. Network security issues attract more and more attention. This paper takes the small and medium-sized enterprises as example, analyzes the relevant theories and technologies of network security, discusses the network security requirements of small and medium-sized enterprises, and clarifies the whole network structure and network topology of small and medium-sized enterprises. And then a more complete enterprise network topology is designed. Through the reinforcement on the physical environment security, network border security, and the network security, the network security level of small and medium-sized enterprise is improved.

Keywords: network security; firewall; topology; design

网络安全在现代生活中越来越受到关注，企业也不例外，许多重要的信息都存储在网上，一旦这些信息泄露出去，不管对个人还是企业都将造成无法估量的损失。究其原因，一方面是网络自身存在的漏洞和安全隐患使得入侵者得逞，另一方面也来自外部的攻击。因此网络安全问题也将面临更严峻的挑战。加强网络安全建设，是关系到企业单位整体形象和利益的大问题，目前每个企业的网络中都存在大量信息，企业许多方面的工作也越来越依赖于网络。一旦网络安全出现问题，就会造成信息的丢失、篡改或者被窃用，给企业带来巨大的损失[1]。本文通过对中小型企业现在的网络状况及网络安全需求进行分析，提出适用于中小型企业网络特点的网络安全体系结构，以满足企业对稳定性、可靠性和安全性的需求。

1　中小型企业信息中心网络安全需求分析

如今是网络大环境时代，网络中潜在的众多威胁因素、Internet 网络协议本身存在的众多缺陷以及企业自身网络架构的漏洞，都将企业的网络安全推上了一个前所未有的战略高度。企业的网络安全需求也是一个不断发展变化的过程，这就需要不断对企业的网络安全需求进行调查分析，总结出可行的网络更改方案，才能保证对企业的网络安全需求具有一定的时效性[2]。因此对中小型企业网络安全体系的构建，应该主要考虑企业网络边界的安

收稿日期：2017-09-01；**修回日期：**2017-10-17

基金项目：国家自然科学基金资助项目(61173190)；陕西省教育厅科研计划资助项目(16JK1236)；陕西省高等教育学会“十三五”规划课题资助项目(XGH1611)；商洛市科学技术研究发展计划项目(SK2016-33)

全、企业内网的安全以及企业内部各部门之间的安全等，主要体现在以下几个方面：

1) 网络安全管理需求：a) 网络安全策略需求方面：虽然企业现在有一些网络安全方面的策略文档，但是过于简单且没有一个完整的体系，缺少一套完整的网络安全策略，不能给整个企业的网络安全工作提供明确的方向和正确的指导。因此需要制定一个完整清晰的安全策略文档体系，定期审视和修订网络安全策略文档，使得信息安全策略有效发布和执行，维护策略的有效性和实用性。b) 企业网络安全组织建设需求方面：建立结构严谨完整的网络安全组织机构，对企业信息安全中心的管理人员进行定期的安全培训，及时掌握一些安全方面的理论和技术。c) 企业网络安全运行管理方面的需求：企业需要建立一套健全的网络安全运行管理体系，引入先进的安全管理理念，制定一套有效实用的网络安全管理方法[3]。

2) 服务器的安全管理需求：增强服务器操作系统的版本，及时发现与修复操作系统漏洞，保证服务器能够正常提供服务，同时全面正确配置服务器的参数，防止因配置不正确引起的漏洞被黑客利用而造成重要信息丢失或受到破坏[4]。

3) 网络管理的需求：需要形成一套清晰完整的管理方案、规范的管理流程、先进的管理工具，能够对网络的安全状况实时地进行监控和检测。

4) 网络访问的可控性需求：构建一套具有访问控制功能的网络安全系统，可以正确辨别访问用户的身份，对访问用户的权限进行合理分配，防止访问用户出现过高权限，从而引起一些重要数据遭到篡改与破坏[5]。

2　中小型企业信息中心网络安全分析

2.1 中小型企业网络安全概述

假设中小型企业在一栋 7 层的办公大楼里，每个部门占据一个楼层。第 7 层是经理部，需要 2 台电脑办公；第 6 层是财务部，需要 100 台电脑办公；第 5 层是人事部，需要 80 台电脑办公；第 4 层是策划部，需要 110 台电脑办公；第 3 层是技术部，需要 200 台电脑，并且在这层设立一个中心管理机房，放置企业中一些外部应用代理服务器、企业内部的重要服务器，如域名系统(Domain Name System，DNS)服务器、文件传输协议(File Transfer Protocol，FTP)服务器和备份服务器等，还需放置核心交换机、汇聚交换机及防火墙等重要的网络安全设备，平时只有网络安全管理人员才拥有进出该中心机房的权限，并且有严格的门禁系统，必须进行刷脸认证；第 2 层是工程部，需要 150 台电脑来办公；第 1 层是销售部，需要 210 台电脑来办公。可以设计见图 1 的网络拓扑图，经过深入实践、广泛调查，该网络拓扑图适用于现今大多数的中小型企业。

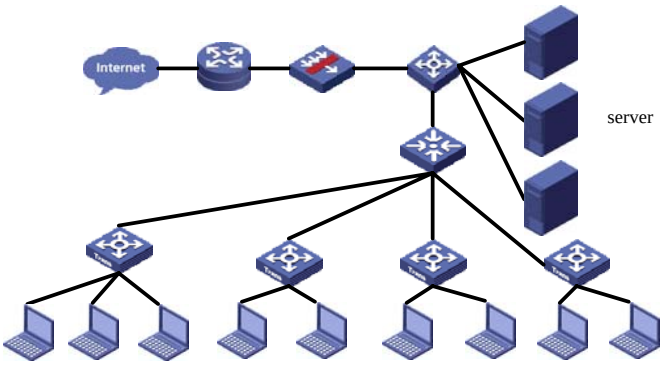

Fig.1 Network topology diagram of small and medium-sized enterprise
图 1 中小型企业网络拓扑图

该网络拓扑图通过一个路由器和外网相连，由这个路由器再连接到防火墙上，分隔外网和内网，并且进行进出数据包的过滤；然后再连接到企业的核心交换机上，核心交换机上连接企业的内部服务器，如邮件服务器和一些备份服务器等；最后再连接到汇聚交换机上，汇聚交换机再接到各部门的二层交换机上[6]。

2.2 存在问题

从图 1 可知，该网络拓扑图虽然能够有效地隔离外网和内网，并且内部也具有一定的备份措施，但还是存在众多的安全漏洞，急需要进一步改进[7]：首先，在与外部相连的路由器上没有配置相应的过滤规则，安全级别较低。其次，边界只配置了防火墙，形式单一，不能很好地进行审查和检测用户安全。最后，企业内部的网络也存在较多漏洞，各部门之间的访问也没有限制，内部的安全管理也比较混乱[8]。

2.3 改进措施

根据企业员工的需求及企业的实际情况重新规划企业的网络拓扑图，提高企业的网络安全等级。与企业的安全管理人员交流及员工的网络安全需求，重新制定方法进行网络安全加固[9]：a) 和外部网相连的路由器可在其入口处配置相应的访问控制列表(Access Control List，ACL)过滤规则，将那些不符合定义规则的数据包初步进行

过滤。b) 在边界防火墙上，将防火墙和虚拟专用网络(Virtual Private Network，VPN)结合起来协同工作，这样可以更好地进行审查和检测，同时 VPN 的搭建可以更好地满足出差在外的员工访问企业的内网，并且通过 VPN 传送的数据都是在一个专用的隧道里面加密传输，不会遭到泄露，提高安全等级[8]。c) 企业内部在各个部门之间划分虚拟局域网(Virtual Local Area Network，VLAN)，这样不同 VLAN 的部门之间不能相互访问，提高内部的安全性[10]。

3 解决方案

经过深入调查研究，以及和众多中小型企业的网络安全管理员及员工交流后，针对图 1 存在的一些问题，提出了改进措施，重新对网络拓扑图进行规划，见图 2，并且制定了网络边界安全及网络内部安全的解决方案，运用一些安全理论技术进行了实现，提高了企业信息中心的网络安全等级[11]。具体改进措施如下：

1) 首先在企业的边界路由器上配置 ACL 访问规则，只有符合规则的数据包才能通过；然后将防火墙和 VPN 技术相结合，进一步提高外出员工访问企业网络的安全性[12]。

2) 在企业内部通过划分 VLAN 来提高各部门之间的相对安全性，再通过单臂路由的配置使得经理可以访问其他部门，但是不同 VLAN 里面的部门之间不能相互访问。同时在防火墙上配置一定的入站规则，控制外部的用户不能访问企业内部的重要服务器，经过授权后只能访问隔离区(Demilitarized Zone，DMZ)区中的应用代理服务器，对内部用户访问这些重要的数据服务器时，制定相应的规则，不能越权访问，确保服务器中数据的安全性[13-14]。

3) 财务处的路由器入口处部署防火墙，定义相应的入站规则，禁止其他部门对财务处的访问[15-16]。

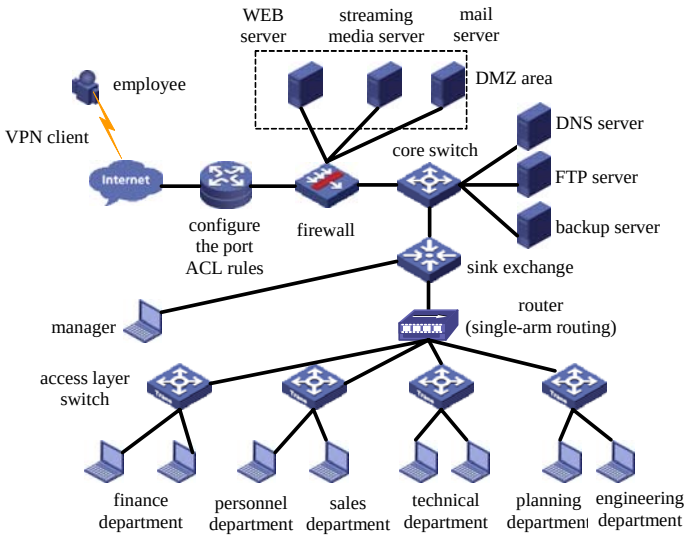

Fig.2 Improved network topology diagram of small and medium-sized enterprise

图 2 改进后的中小型企业网络拓扑图

4 结论

随着网络的广泛应用，网络安全问题日益凸显，企业的网络安全策略也应该动态变化，要逐渐从被动防御转变为主动检测和攻击，安全防御技术与策略也要及时更新，逐渐向智能化方向发展，提高安全防护能力。本文探讨了中小型企业网络安全系统需求，以一栋办公大楼的中小型企业为研究对象，深入研究了中小型企业网络安全需求和网络拓扑图，建立相应的安全管理机制，并重新构建中小型企业的网络安全环境方案，提高了中小型企业的网络安全等级。运用先进的网络安全技术理论对中小型企业的网络安全进行加固，对中小型企业的网络安全建设具有一定的实际应用意义。

参考文献：

[1] 金俊才,许超超. 企业级服务器虚拟化性能评估方法[J]. 计算机系统应用, 2015,24(7):1-7. (JIN Juncai,XU Chaochao. Performance evaluation of the enterprise-level virtualization[J]. Computer Systems Applications, 2015,24(7):1-7.)

[2] 朱建明,宋彪,黄启发. 基于系统动力学的网络安全攻防演化博弈模型[J]. 通信学报, 2014,35(1):54-61. (ZHU Jianming, SONG Biao,HUANG Qifa. Evolution game model of offense-defense for network security based on system dynamics[J]. Journal on Communications, 2014,35(1):54-61.)

[3] 文志诚,陈志刚,唐军. 基于时间序列分析的网络安全态势预测[J]. 华南理工大学学报(自然科学版), 2016,44(5):137-143. (WEN Zhicheng,CHEN Zhigang,TANG Jun. Prediction of network security situation on the basis of time series analysis[J]. Journal of South China University of Technology(Natural Science Edition), 2016,44(5):137-143.)

[4] 周诚,李伟伟,莫璇. 一种网络安全脆弱性评估方法[J]. 江苏大学学报(自然科学版), 2017,38(1):68-77. (ZHOU Cheng, LI Weiwei,MO Xuan. A assessment method of network security vulnerability[J]. Journal of Jiangsu University(Natural Science Edition), 2017,38(1):68-77.)

[5] 王栋,陈传鹏,颜佳. 新一代电力信息网络安全架构的思考[J]. 电力系统自动化, 2016,40(2):6-11. (WANG Dong,CHEN Chuanpeng,YAN Jia. Pondering a new-generation security architecture model for power information network[J]. Automation of Electric Power Systems, 2016,40(2):6-11.)

[6] 芦荻,商慧琳. 基于反导作战环的装备作战网络能力评估[J]. 太赫兹科学与电子信息学报, 2016,14(3):372-377. (LU Di,SHANG Huilin. Assessment of equipment operation network capability based on the anti-missile operation loops[J]. Journal of Terahertz Science and Electronic Information Technology, 2016,14(3):372-377.)

[7] 黄雁,邓元望,王志强. 可入侵检测的移动 Ad Hoc 网络安全综合评价[J]. 中南大学学报(自然科学版), 2016,47(9):3031-3039. (HUANG Yan,DENG Yuanwang,WANG Zhiqiang. Comprehensive evaluation of security of mobile ad hoc network with intrusion detection[J]. Journal of Central South University(Natural Science Edition), 2016,47(9):3031-3039.)

[8] 陈兴蜀,曾雪梅,王文贤. 基于大数据的网络安全与情报分析[J]. 工程科学与技术, 2017,49(3):1-11. (CHEN Xingshu, ZENG Xuemei,WANG Wenxian. Big data analytics for network security and intelligence[J]. Advanced Engineering Sciences, 2017,49(3):1-11.)

[9] 赵冬梅,李红. 基于并行约简的网络安全态势要素提取方法[J]. 计算机应用, 2017,37(4):1008-1013. (ZHAO Dongmei, LI Hong. Approach to network security situational element extraction based on parallel reduction[J]. Computer Systems Applications, 2017,37(4):1008-1013.)

[10] 孙琳,潘登,刘获. 基于预约诊疗模式下的医院网络安全设计[J]. 现代电子技术, 2017,40(3):82-84. (SUN Lin,PAN Deng, LIU Di. Design of hospital network security based on reservation and treatment mode[J]. Modern Electronics Technique, 2017,40(3):82-84.)

[11] 屈正庚. 基于信息中心的运营监控模型设计[J]. 太赫兹科学与电子信息学报, 2015,13(2):327-331. (QU Zhenggeng. Design of operation monitoring model based on information center[J]. Journal of Terahertz Science and Electronic Information Technology, 2015,13(2):327-331.)

[12] 杨乐. 分散控制系统信息安全方案探讨[J]. 石油化工自动化, 2017,53(3):1-4. (YANG Le. Discussion on information security design of distributed control system[J]. Automtion in Petro-Chemical Industry, 2017,53(3):1-4.)

[13] 蒋笑冰. 铁路移动办公系统安全防护方案的研究[J]. 铁路计算机应用, 2015,24(9):22-26. (JIANG Xiaobing. Security protection scheme for railway mobile office automation system[J]. Railway Computer Application, 2015,24(9):22-26.)

[14] 张爱玲. 移动运营商网络安全管理平台架构分析与探索[J]. 科技通报, 2017,33(2):90-94. (ZHANG Ailing. Mobile operator's network security management platform architecture analysis and exploration[J]. Bulletin of Science and Technology, 2017,33(2):90-94.)

[15] 何雪海,黄明浩,宋飞. 网络安全用户行为画像方案设计[J]. 通信技术, 2017,50(4):789-794. (HE Xuehai,HUANG Minghao, SONG Fei. User behavior profiling scheme for network security[J]. Communications Technology, 2017,50(4):789-794.)

[16] 罗福强,李瑶,范展源. 灾害与突发事件 ICU 大数据平台的安全设计[J]. 计算机技术与发展, 2016,26(10):69-72. (LUO Fuqiang,LI Yao,FAN Zhanyuan. Safety design of ICU big data platform for disaster and sudden event[J]. Computer Technology and Development, 2016,26(10):69-72.)

作者简介：

屈正庚(1982-)，男，陕西省西乡县人，硕士，副教授，主要研究领域为协同设计与网络控制、电子商务.email:quzhenggeng@163.com.

吕　鹏(1993-)，男，陕西省千阳县人，在读硕士研究生，主要研究领域为数据库技术.