学校编码：10384　　分类号_____密级_____

学号：X2009221043　　UDC_____

厦门大学

工　程　硕　士　学　位　论　文

厦门工学院校园网网络方案安全设计与实施

Xiamen Institute of Technology Campus Network Security Design Scheme and Implementation

张勇

指导教师姓名：　杨晨晖 教授

专　业　名　称：　计算机技术

论文提交日期：　2014 年　月

论文答辩日期：　2014 年　月

学位授予日期：　2014 年　月

答辩委员会主席：_____

评　　阅　　人：_____

2014 年　　月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

网络化、信息化已成为现代社会的一个重要特征。校园网为高校教学、管理、信息交流和通信等提供网络应用环境，已然成为高校教育信息化的基础设施和重要标志。高校校园网作为互联网人数众多，架构复杂程度高的网络代表之一，保障校园网网络安全稳定可靠运行成为网络设计和运维人员最为关心的核心问题。随着校园网承担的科研、教学任务的急剧增加，面临的安全威胁和攻击也越来越多，所以构建一个安全稳定的网络系统势在必行。

本文在把握校园网网络安全管理系统的整体结构基础上，结合当前网络安全主要的技术，详细分析了校园网络安全的要求，从校园网安全，网络审计要求、统一准入认证等方面详细分析了校园网络安全的要求。

基于将原有校园网网络外包独家垄断经营，变更为移动、电信、联通三家运营商同时进入校园网的架构模式。在此基础上，依据网络设计综合、整体原则、可用性原则、分步分级实施原则、动态管理原则等方面的设计原则，本文提出网络设计思路从连通性转变为安全为中心，从远程接入设计、内部网络安全设计、边界安全设计、统一安全运维管理设计等方面，利用防火墙、防毒墙、IDS、VPN、运维拓扑管理系统等安全技术和产品协同工作，来保障校园网安全运转。

本文在最后基于工学院校园网，对部分安全功能进行测试验证，并提出本次项目实施过程中未能解决和需要改进的问题。

关键词： 网络安全　防火墙　IDS　校园网

Abstract

Networking, information technology has become an important feature of modern society , with the rapid development of network technology , computer network has become the life work of an essential part of learning . Campus Network as a large number of Internet , one of the high complexity of the network architecture representative of the campus network security and reliable operation of the network security issues become the core of the network design and operation and maintenance personnel are most concerned about . With the dramatic increase in campus networks for research , teaching tasks facing security threats and attacks are increasing, so to build a secure and stable network system is imperative.

In this paper, basic grasp of the overall structure of campus network security management system , combined with the current network security key technical , detailed analysis of the campus network security requirements, from the campus network security , a detailed analysis of network audit requirements , and other aspects of a unified access authentication campus network security requirements.

Based on the original campus network outsourcing exclusive monopoly , change to Mobile, Telecom, China Unicom three operators simultaneously into the campus network architecture model. On this basis , according to a comprehensive network design , step by step implementation of the design principles of hierarchical principle , this paper presents the design ideas from network connectivity into a security center, from remote access design internal network security design, border security design , operation and maintenance of a unified security management and other aspects of the design , the use of firewall, antivirus wall , IDS, VPN, topology management system, operation and maintenance of security technologies and products work together to protect the safe operation of the campus network .

In this paper, based on the Institute campus at the end , on the part of the test to verify the safety features and make the process failed to resolve the issue and the need to improve the implementation of this project .

Keywords: network security firewall IDS campus network

目录

第一章　绪论 1
1.1 课题研究背景及意义 1
1.2 课题的主要研究内容 2
1.3 课题结构安排 2
第二章 网络安全综述 4
2.1 网络安全概念 4
2.2 网络安全关键技术 4
2.2.1 Firewall 技术 4
2.2.2 IDS 技术 6
2.2.3 VPN 技术 7
2.2.4 VLAN 技术 8
第三章 校园网安全设计需求分析及目标 10
3.1 校园网安全需求分析 10
3.2 校园网安全方案设计原则 10
3.3 校园网安全平台设计目标 12
3.3.1 按安全需求划分不同区域 12
3.3.2 关键路径安全防护检测 12
3.3.3 用户上网行为识别和管理 13
3.3.4 统一网络安全运维管理及日志审计 13
第四章 校园网网络安全方案设计概述 14
4.1 网络安全方案设计概述 14
4.2 校外远程访问设计方案 14
4.2.1 SSL VPN 部署概述 14
4.2.2 SSL VPN 部署优点 15
4.2.3 SSL VPN 部署模式 15
4.3 边界网络安全设计方案 16
4.3.1 设计方案概述 16
4.3.2 设计方案部署 17
4.4 内部网络安全设计方案 18
4.4.1 内部网络安全设计概述 19
4.4.2 内部网络安全设计实施 20

4.5 统一安全运维管理设计方案 20
第五章 工学院网络安全体系方案实施 21
5.1 工学院校园网网络组成及现状 21
5.2 工学院校园网网络层次化模型的设计 22
5.2.1 接入层 22
5.2.2 汇聚层 25
5.2.3 核心层 27
5.3 应用设备选型及设备性能 29
5.3.1 TTnet 应用层流量分析控制系统 29
5.3.2 锐捷应用性能管理系统 33
5.3.3 RIIL 运维管理系统 34
第六章 工学院 SAM 计费管理认证系统的安全设计与实施 37
6.1 计费管理认证需求分析 37
6.2 安全集群硬件环境 37
6.3 计费管理认证解决方案概述 42
6.4 802.1X 认证设计实现方案 46
第七章 校园网结构的性能测试与分析 47
7.1 安全日志审计测试 47
7.2 虚拟专用网 VPN 测试 49
7.3 IDS 功能测试 52
7.4 深信服上网行为管理设备测试 55
7.5 接入交换机安全通道功能测试 55
7.6 接入交换机逃生功能测试 57
第八章 总结与展望 60
8.1 项目实施运行中存在的几个问题 60
8.2 研究展望 60
参考文献 62
致 谢 65

Contents

Chapter1 Introduction 1

1.1 The research background and the significance 1

1.2 The main contentsr 2

1.3 The main research contents of this topic 2

Chapter2 Network security summary 4

2.1 Network security concepts 4

2.2 Network security key technology 4

2.2.1 Firewall technology 4
2.2.2 IDS technology 6
2.2.3 VPN technology 7
2.2.4 VLAN technology 8

Chapter3 Security requirements analysis and design goals 10

3.1 Campus network security needs analysis 10

3.2 Campus network security design principles 10

3.3 Campus network security platform designed 12

3.3.1 Divided by the security needs of different regions 12
3.3.2 Detection protection network critical path 12
3.3.3 Conduct effective identification and management 13
3.3.4 Unified security operation management and behavioral audit 13

Chapter 4 Campus network security design overview 14

4.1 Overview of network security solutions designed 14

4.2 Remote access design 14

4.2.1 SSL VPN design overview 14
4.2.2 SSL VPN design features 15
4.2.3 SSL VPN network deployment design 15

4.3 Design border security 16

4.3.1 Overview border security design 16
4.3.2 The design of the deployment of border security features 17

4.4 The internal network security design 18

4.4.1 Overview of network security design 19
4.4.2 The implementation of internal network security design 20

4.5 The unified security management scheme 20

Chapter 5 Implementing network security system solutions 21

5.1 Composition and college campus network status 21

5.2 Institute of Technology campus network hierarchical model design 22

5.2.1 Access Layer 22
5.2.2 Convergence layer 25
5.2.3 Core layer 27

5.3 Application of equipment selection and equipment performance 29

5.3.1 TTnet application layer traffic analysis and control system 29
5.3.2 Ruijie application performance management system 33
5.3.3 RIIL management system 34

Chapter 6 Design and implementation of authentication system 37

6.1 User authentication requirements analysis 37

6.2 Security cluster hardware environment 37

6.3 User authentication solution overview 42

6.4 802.1X Authentication design implementation 46

Chapter 7 Performance measurement and analysis 47

7.1 Security log audit test 47

7.2 SSL VPN function test 49

7.3 IDS function test 52

7.4 SANGFOR management application control function test 55

7.5 Access switch secure channel functional test 55

7.6 Access switch escape function test 57

Chapter 8 Conclusion and the prospect 60

8.1 Project run several problems exist 60

8.2 Prospect 60

References 62

Acknowledgements 65

第一章 绪论

1.1 课题研究背景及意义

随着信息化步伐的日益加快，各式各样的商业、金融活动都通过互联网进行交易，Internet 技术被广泛应用于各个社会的层面和行业，大大丰富了人们的生活和娱乐，网络成为诸多人工作生活中及其重要的组成部分。自 20 世纪 90 年代 Internet 进入商界，快速的发展态势，当前已成为推动世界经济发展、社会进步非常重要的基础设施之一。2014 年 1 月 16 日，中国互联网络信息中心（CNNIC）在京发布第 33 次《中国互联网络发展状况统计报告》显示，截止到 2013 年 12 月，中国的网民规模达 6.18 亿，互联网普及率为 45.8%，较 2012 年底提升 3.7 个百分点[1]。随着不断膨胀的网络用户，基于网络的网上银行、电子商务、虚拟货币以及其它各种新兴的网上应用业务的迅猛发展，互联网安全性变得更为重要。

网络技术的飞速发展，数字校园、信息化教育已成为当前教育发展的前进方向，校园网承担着高校教学工作、科学研究、行政管理和对外交流等各式各样的角色，发挥的作用越来越大。大多数高校都建立了自己的校园网，便于提高工作效率，加快信息处理，资源共享，降低工作强度等等。校园网络一方面提供了便利，但另一方面也带来了教师和学生网络安全问题，例如非法登录校园网、进行非法网站的访问、非法网站登录访问和使用内嵌病毒软件等，这可能导致高校校园网络安全事故，甚至系统崩溃，更为严重点将会影响校园网的日常运行，且随着校园 E 卡通的推广，网络安全也涉及到校园财务安全。因此，校园网网络安全问题已经成为影响国家网络信息化发展和教育事业发展的重要因素[2]。

此外,伴随着网络规模迅猛发展,网络架构的也变得愈来愈庞大,相关业务和网络应用不断的发展也对网络性能提出更高的要求。从而网络安全管理影响着网络今后的发展方向,网络安全技术已经成为了网络技术发展中的重要技术要素之一[3]。如果没有一个集成化的、高效的校园网网络安全管理体系对校内网络进行安全管理，网络管理工作人员就不能对校园网网络安全情况做到了如指掌，校内网网络安全也就难以得到保障,更别说保证校园网络安全稳定运行。所以,当前迫切需要一种安全系统的校园网安全解决方案，可以实用、高效、安全的保障校园

网的持续稳定运行，使高校业务得以顺利开展。

1.2 课题的主要研究内容

本文研究的是以工学院作为设计对象，设计的高校网络安全体系应具有可扩展性强、安全稳定、冗余备份、高效快捷的优点。本文通过对工学院网络安全现状分析，结合当前现有的安全技术，研究分析高校网络安全需求以及设计的基本原则，从远程的访问安全、边界安全、内部安全、上网行为安全审计、统一运维拓扑管理等方面，并有针对性的对原有旧的系统进行升级，系统地论述了高校网络安全体系的设计与实施。

1.3 课题结构安排

本文基于对目前校园网络存在或即将面临的安全问题展开详细解剖的基础之上，深入研究当前的最新网络安全技术、工具软件的功能和优势略势，并具体分析了网络安全技术在校园网络中的各种具体应用，并以工学院为研究对象，探讨了如何使用当前各种先进的网络安全技术，来保障校园网络高效、稳定、安全的运作，并结合本校的实际情况，给出解决网络安全问题的具体实例，本文重点研究以下几个方面的问题：

第一章：绪论。主要是介绍课题选题研究的背景与意义，课题研究的主要内容以及后续各章节的具体内容设计安排。

第二章：网络安全综述。主要对当前网络安全的技术进行了综述，对网络安全技术的发展趋势做个相关的描述。

第三章：校园网网络安全需求分析及设计目标。这章先深入分析当前高校校园网网络安全需求，然后依据安全需求，有针对性提出了校园网网络方案的设计原则及设计最终目标。

第四章：校园网网络安全方案设计概述。本章从远程安全接入设计、边界安全设计、内部网络安全设计、上网行为审计设计、统一安全运维管理设计等五个方面详细阐述了方案的设计。

第五章：工学院网络安全体系方案实施。本章以工学院为实际案例，对网络安全实现、安全设备选型、基本数据配置进行了阐述，是对前面章节设计目标和设计的实现。

第六章：工学院用户认证系统的安全设计与实施。本章节以工学院为实际案

例，针对终端用户安全管理进行分析和实施。

第七章：校园网结构的性能测试与分析。本章节主要是针对系统实施过程中一些功能和系统性能进行相关的测试和验证分析。

第八章：总结和展望。本章对本文的研究过程、内容进行概括总结，并提出项目实施过程存在的问题，并展望未来网络的发展。

第二章 网络安全综述

2.1 网络安全概念

网络安全是一门涉及到计算机科学技术、网络技术、通信技术、信息安全技术、密码技术、应用数学、数论和信息论等多种学科的综合性学科[4]。网络安全是保护加载数据的硬件、软件和网络系统，不会因偶然或变化的因素而造成数据泄露损坏，从而保证系统可以高可靠高稳定性地运行，提供不中断的服务保障网络的安全。从其本质上来讲，网络安全其实就是网络的信息安全，从广义来说，网络安全研究领域是涉及到网络信息的完整性、保密性、真实性、可用性和可控性的相关技术及理论。但不同对象对网络安全具体的含义会有不同的理解，在网络的使用者看来，当然是希望商业秘密、个人安全、个人隐私等相关私有信息能够完整、真实、保密地在网络上进行传输和存储，并能够避免非授权人员利用各种非法手段对信息进行窃取、篡改，损害到网络使用者的既有利益，但是对于具体的网络管理和实施安装维护人员来说，他们更希望能够保证网络及其网络中的资源能被正常访问和操作，网络不被攻击、不受病毒感染、网络资源不要受到非法用户占用和控制[5]。

2.2 网络安全关键技术

2.2.1 Firewall 技术

防火墙(Firewall)技术是能够提供网络安全保障的软硬件构成的系统。其原理是按事先约定的配置和规则，监测过滤进出内外网的信息，保障内部网络敏感数据的安全[6]。在网络中，所谓防火墙就是一种能够将内部网络与公众访问网络（如 Internet）分开的方法，它实际上是一种物理隔离的技术。

防火墙也就是计算机网络系统中，工作在两个甚至更多个网络之间的一种硬件设备。一般的防火墙体系网络系统结构如图 2-1 所示，从图中明显可以看得出网络防火墙是内、外网络数据传输的必经之路。

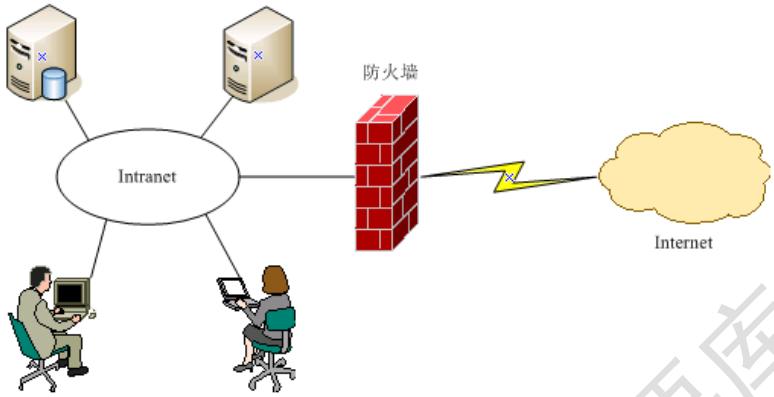

图 2-1 防火墙网络体系结构

按其工作方式可以将防火墙技术分为两种类型：包过滤型防火墙（IP Filtering Firewall）和代理服务（Proxy Server）型防火墙。

1）包过滤型防火墙（IP Filtering Firewall）

包过滤型防火墙又被叫作网络级防火墙，是基于数据包过滤的防火墙，其主要工作在网络层。防火墙通过检查分析每个数据包的 IP 地址，所采用的通信协议和端口号等等来判断是否允许放行数据包[7]。它有以下三种类型：

静态包过滤防火墙，基于预设好的数据包的报头信息，运用过滤规则筛选所有通过的数据包，从而确定是否能够与防火墙其中一条包过滤规则相匹配；

动态包过滤防火墙，在改进静态包过滤所存在的问题的基础上，比如说遇到利用动态端口的协议就会发生一些困难，如 FTP 应用，防火墙不能够判断哪些端口需要打开，但用户又非常希望应用到此服务，这就需要将所有可能用到的端口全部打开，而往往就是这个非常宽的范围，会给黑客或黑客工具带来可乘之机，因此在此基础上发展就有动态包过滤防火墙；状态检测利用检查应用程序信息（如 FTP 应用的端口号和密码）来判断此端口是否需要临时打开，当信息传输结束后，此端口又马上转变为关闭的状态[8]。

状态检测防火墙，状态就是网络的连接情况，防火墙通过连接数据包不同标志位的参数变化来表示状态的改变，根据规则表和状态的变化来对数据包进行检查。

2）代理服务（Proxy Server）型防火墙

代理服务型防火墙又被称作为应用级的网关，是对包过滤防火墙的补充，其主要工作在应用层。使用代理服务器从而达到隐藏内部网络结构的作用是其最关键技术。防火墙需要为每种服务都建立一个代理，内外网络均没有直接的服务连接，连接时都需要通过相应的代理审核完成之后才能够再转发。优点就是可以对网络连接的深层次内容进行相应监控，从而阻断内外部网络的连接，最终实现网络的相互间屏蔽。缺点是处理速度慢，很容易成为网络运行的瓶颈。

2.2.2 IDS 技术

入侵检测技术（IDS）是通过收集并分析计算机网络或计算机的系统中若干关键节点的信息，从而对入侵行为作出相应的检测，如图 2-2。IDS 是计算机系统中有效的防范手段，对正常和无用的系统行为提供识别技术，同时对内外部攻击实时保护，也能对传输中的信息监控，发现基于网络的攻击[9]。

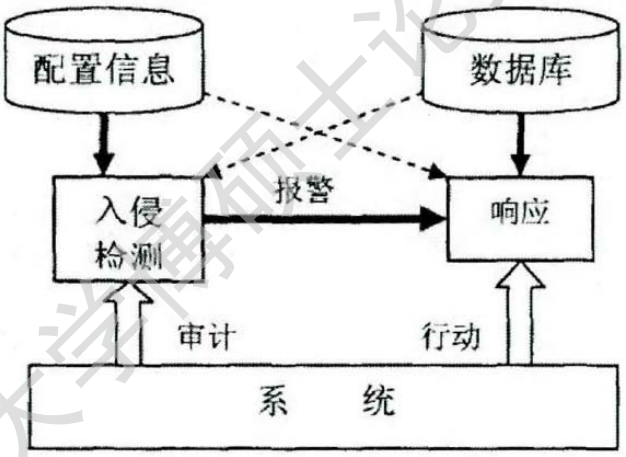

图 2-2 简单入侵检测系统原理图

按照系统结构和数据来源分类，可以将入侵检测分为基于主机、基于网络和分布式入侵检测[10]。

1）基于主机的入侵检测系统 HIDS，HIDS 检测目标的主要是主机系统和系统本地用户，原理是根据主机的审计数据和系统的日志从而发现可疑事件，入侵检测系统可以运行在被检测的主机或单独的主机上。此系统依赖于系统日志或审计数据的准确性、完整性以及安全事件的定义。此系统一般应用在系统服务器、终端用户机器和工作站上。

2）基于网络的入侵检测系统 NIDS，部署在网络系统的关键节点，主要用来