湖南电子科技职业学院
HUNAN VOCATIONAL COLLEGE OF ELECTRONIC AND TECHNOLOGY

产品设计	方案设计	工艺设计
	√	

信息工程学校

毕 业 设 计

题目：益阳职业中专学校校园网安全分析与解决方案

学生姓名　陈嘉俊

学生学号　010425171765

班级名称　G32208 班

专业名称　计算机网络技术

指导教师　龙佳

2025 年 05 月

毕业设计真实性承诺及指导教师声明

本人郑重声明：所提交的毕业设计是本人在指导教师的指导下，独立进行研究工作所取得的成果，内容真实可靠，不存在抄袭、造假等学术不端行为。除设计中已经注明引用的内容外，本设计不含其他个人或集体已经发表或撰写过的研究成果。对毕业设计的研究做出重要贡献的个人和集体，均已在设计中以明确方式标明。如被发现设计中存在抄袭、造假等学术不端行为，本人愿承担相应的法律责任和一切后果。

学生（签名）：陈嘉修　日　期：2025.5.11

指导教师关于学生毕业设计真实性审核的声明

本人郑重声明：已经对学生毕业设计所涉及的内容进行严格审核，确定其成果均由学生在本人指导下取得，对他人成果的引用已经明确注明，不存在抄袭等学术不端行为。

指导教师（签名）：[illegible]　日　期：2025.5.16

（注：本页学生和指导教师须亲笔签名。）

目 录

一、益阳职业中专学校园网

（一）益阳职业中专学校网络建设背景

益阳职业中专学校的校园网建设旨在为教育教学提供有力支持，推动学校教育现代化进程。学校充分考虑教育教学的实际需求与经济承受能力，秉持统一规划、分步实施的原则，有序推进校园网建设。通过严格规范校园网建设及软件开发标准，确保信息化校园的整体建设规划与管理要求得以落实。

在校园网建设过程中，学校高度重视教师、技术人员、管理人员及行政人员的多层次培训，致力于打造一支能够充分发挥校园网效益的应用团队、教学软件开发团队以及保障校园网持续稳定运行的软硬件管理团队。学校积极开发和推广教育教学软件，建设信息资源库，以提升校园网的使用效益。

1、建设背景和现状

益阳职业中专学校在计算机辅助教学领域起步较早，已建成大规模的计算机实验室，拥有上千台计算机设备。然而，目前各系部各自组建内部网络，导致软件平台和硬件设备缺乏统一标准，网络管理分散，难以实现资源的高效整合与共享，这在一定程度上制约了校园网整体效益的发挥。

2、建设需求分析

学校校园网建设的核心目标是服务于教育教学，促进教育现代化。基于教育教学的实际需求和经济条件，学校将遵循统一规划、分步实施的原则，有计划、有重点地推进校园网建设。通过严格规范校园网建设及软件开发标准，确保信息化校园的整体建设规划和管理要求得到有效落实。

学校在计算机辅助教学方面积累了丰富的经验，建立了大规模的计算机实验室，拥有上千台计算机设备。但目前各系部各自为政的网络建设模式，使得软件平台和硬件设备参差不齐，网络管理分散，难以实现资源的高效整合与共享。这不仅影响了校园网的整体效益，也给学校的信息化管理带来了诸多挑战。因此，学校亟需对现有网络进行优化升级，统一网络架构，规范设备标准，加强集中管理，以实现资源的高效共享和网络的稳定运行，为教育教学提供更有力的支持。

（二）益阳职业中专学校安全隐患介绍

互联网自 1969 年 ARPANet 诞生并最初用于军事目的以来，于 1993 年开始广泛应用于商业领域。如今，随着计算机技术的飞速发展，其应用领域不断拓展，尤其在教育机构中，校园网已成为教学、办公、科研以及资源共享的重要工具。然而，校园网在带来诸多便利的同时，其开放性、共享性、广泛性和复杂性也引发了一系列令人担忧的网络安全问题，使得网络安全成为当前校园网络建设中亟待解决的关键课题。无论我们是否愿意承认，只要接入 Internet，网络就不可避免地面临被攻击的风险。因此，在网络开放性和共享性的基础上，如何确保校园网络的安全性，抵御入侵和防范网络攻击，已成为校园网络建设中不可忽视的重要任务。

1、校园网网络安全的概述

随着网络技术的飞速发展，如今大多数学校都已建成并投入使用了校园网。校园网的广泛应用极大地加快了信息处理速度，提高了工作效率，实现了资源共享，为学校的教育教学和管理工作带来了诸多便利。然而，在享受网络带来的便利的同时，网络安全问题也逐渐凸显，成为校园现代化进程中的一大隐患，如同一颗深埋的定时炸弹，随时可能引发严重后果。

近年来，诸如 2016 年的“震荡波”“冲击波”以及 2006 年的“熊猫烧香”等病毒事件，虽然未对校园网络造成毁灭性打击，但也足以敲响网络安全的警钟。这些事件充分暴露了网络安全的重要性，促使学校必须将网络安全纳入重要议事日程。要有效解决网络安全问题，首先需要深入了解网络的基本结构和功能。益阳职业中专学校的网络结构拓扑图如图 1.1 所示：

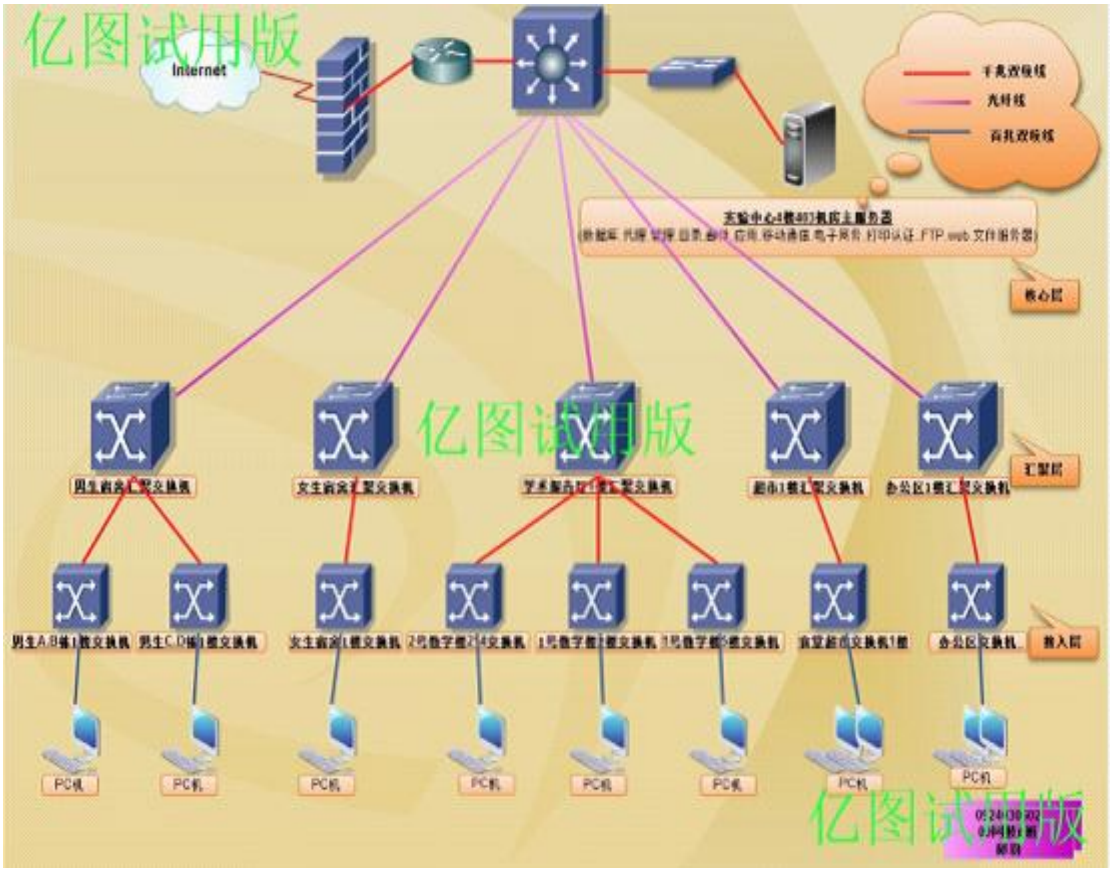


图 1.1　校园网络结构拓扑图

通过对学校网络现状和安全需求的深入分析，我们发现当前校园网在安全方面存在以下主要问题：

（1）网络架构分散，缺乏统一管理

由于各系部自行组建内部网络，导致网络架构分散，缺乏统一的规划和管理。这种分散的网络架构不仅增加了管理难度，也使得网络安全策略难以统一部署和实施，容易出现安全漏洞。

（2）软件平台和硬件设备参差不齐

各系部采用的软件平台和硬件设备种类繁多，缺乏统一标准。这不仅增加了网络维护的复杂性，也使得不同网络之间的兼容性和互操作性面临挑战，容易引发安全问题。

（3）网络安全意识薄弱

部分师生和管理人员对网络安全的重要性认识不足，缺乏基本的网络安全知识和防范意识。这使得学校网络容易受到外部攻击和内部误操作的影响，增加了网络安全风险。

（4）缺乏有效的安全防护措施

学校网络在防火墙、入侵检测、病毒防护等方面的安全防护措施相对薄弱，难以有效抵御外部攻击和病毒入侵。同时，学校尚未建立完善的网络安全应急响应机制，一旦发生安全事件，难以快速有效地进行处理。

针对上述问题，学校需要采取一系列措施来提升校园网的安全性，确保网络的稳定运行和信息安全。具体措施包括：

2、网络安全优化建议

（1）统一网络架构，加强集中管理

学校应制定统一的网络建设标准，对全校网络进行统一规划和管理。通过整合各系部的网络资源，构建集中化的网络架构，实现资源的高效共享和统一调度。同时，建立完善的网络管理制度，明确各部门在网络管理中的职责，确保网络安全策略的有效实施。

（2）规范软件平台和硬件设备标准

学校应制定统一的软件平台和硬件设备标准，规范各系部的网络建设。通过统一设备型号和软件版本，降低网络维护的复杂性，提高网络的兼容性和互操作性。同时，定期对设备进行更新和升级，确保网络设备的安全性和可靠性。

（3）加强网络安全教育，提高师生安全意识

学校应定期开展网络安全培训，提高师生和管理人员的网络安全意识。通过组织专题讲座、培训课程和宣传活动，普及网络安全知识，增强师生对网络攻击、病毒入侵等安全威胁的防范意识。同时，制定网络安全行为规范，引导师生合理使用网络资源，避免因不当操作引发安全问题。

（4）完善安全防护体系，提升网络安全防护能力

学校应加强网络安全防护措施，构建多层次的安全防护体系。在防火墙、入侵检测、病毒防护等方面加大投入，部署先进的安全设备和软件，提升网络的抗攻击能力和病毒防护能力。同时，建立完善的网络安全应急响应机制，制定应急预案，定期进行演练，确保在发生安全事件时能够快速有效地进行处理，最大限度降低损失。

3、网络安全的内涵

网络安全涵盖网络系统的硬件、软件以及数据的全方位保护，旨在防止这些关键要素遭受意外或恶意的破坏、篡改与泄露。它确保网络系统能够连续、可靠且稳定地运行，同时保障网络服务的不间断性。网络安全的定义并非一成不变，在不同的应用场景和环境中有着多样化的解读。

（1）运行系统安全：这一层面聚焦于保障信息处理与传输系统的安全性。它涉及计算机系统机房环境和传输环境的法律保护，计算机硬件架构的安全设计，硬件系统的稳定运行，操作系统与应用软件的安全性，数据库系统的防护，以及电磁信息泄露的防范等多个方面。

（2）网络系统信息安全：主要围绕用户身份验证、权限控制、数据访问权限管理、安全审计、安全问题追踪、计算机病毒防范以及数据加密等关键环节展开，确保网络系统中的信息安全无虞。

（3）网络信息传输安全：关注信息传播过程中的安全性，包括信息过滤和不良信息拦截等，防止有害信息在网络中扩散。

（4）网络信息内容安全：这是狭义上的“信息安全”，着重保护信息的机密性、真实性和完整性，本质上是为了维护用户的利益和隐私。

4、威胁网络安全的不安全因素剖析

（1）网络开放性引发的安全挑战

Internet 的开放性以及诸多其他因素，使得网络环境下的计算机系统面临着诸多安全问题。尽管各种安全机制、策略、管理和技术不断被研究和应用，但在现有安全工具和技术的加持下，网络安全依然存在诸多隐患，主要体现在以下几点：

A. 安全机制的局限性：以防火墙为例，虽然它是一种有效的安全工具，能够隐藏内部网络结构，限制外部网络对内部网络的访问，但对于内部网络之间的访问，防火墙往往无能为力。因此，针对内部网络之间的入侵行为以及内外勾结的入侵行为，防火墙很难察觉和防范。

B. 安全工具使用的人为因素：安全工具能否达到预期效果，在很大程度上取决于使用者，包括系统管理者和普通用户。不恰当的设置会引入安全隐患。例如，Windows XP 在合理配置后可以达到 C 级安全性，但很少有人能够对其安

全策略进行合理设置。尽管可以通过静态扫描工具检测系统配置的合理性，但这些工具大多基于默认的安全策略进行比较，在具体应用环境和特定需求下，很难判断设置的正确性。

C. 系统后门的隐蔽性：防火墙很难防范系统后门带来的安全问题。例如，IIS 服务器 4.0 以前版本中存在的 ASP 源码问题，是设计者留下的后门，攻击者可以通过浏览器轻松获取 ASP 程序的源码，进而收集系统信息并发起攻击。对于此类入侵行为，防火墙难以察觉，因为其访问过程与正常的 WEB 访问相似，唯一的区别在于请求链接中多了一个后缀。

（2）网络安全的主要威胁因素

A. 软件漏洞：任何操作系统或网络软件都不可能完美无缺，漏洞的存在使计算机系统面临巨大风险。一旦接入网络，这些漏洞将成为攻击者的突破口。

B. 配置不当：错误的安全配置会引入安全漏洞。例如，防火墙软件配置错误将使其失去防护作用。某些网络应用程序启动时会打开一系列安全缺口，其捆绑的应用软件也会被启用。除非用户禁止或正确配置这些程序，否则安全隐患始终存在。

C. 安全意识薄弱：用户选择弱密码、随意转借账号或与他人共享账号等行为，都会对网络安全构成威胁。

D. 病毒威胁：计算机病毒是数据安全的头号敌人，它是插入计算机程序中的一组指令或代码，具有传染性、寄生性、隐蔽性、触发性和破坏性等特点，能够破坏计算机功能和数据，影响软件和硬件的正常运行。因此，加强病毒防范刻不容缓。

通过以上措施的实施，益阳职业中专学校将能够有效提升校园网的安全性，确保网络的稳定运行和信息安全，为教育教学和学校管理提供更加可靠的信息化支持。

二、益阳职业中专学校园网网络安全隐患分析

随着高校规模的持续扩张以及新校区或合并校区的不断建设，校园网的规模日益庞大，上网地点愈发分散，网络监管难度显著增加，上网行为也逐渐变得不够规范。这些因素共同导致校园网络在使用过程中面临着诸多安全隐患。

（一）校园网安全存在的缺陷

1、网络协议的固有缺陷

网络环境本质上是开放的，而 TCP/IP 协议作为一种通用协议，通过 IP 地址标识网络节点，并基于此进行用户认证与授权。然而，该协议的最大弊端在于缺乏对 IP 地址的保护机制，无法有效验证源 IP 地址的真实性，这正是 TCP/IP 协议不安全的根本原因。基于这一缺陷，常见的攻击手段包括源地址欺骗、IP 欺骗、源路由选择欺骗、路由选择信息协议攻击、SYN 攻击等。

2、网络结构、配置与物理设备的不安全性

互联网最初仅服务于少数可信用户，设计时未充分考虑安全威胁，导致互联网及其连接的计算机系统存在大量安全漏洞。在实际使用中，由于连接的计算机硬件种类繁多，部分厂商可能将未经严格测试的产品推向市场，进一步增加了安全隐患。此外，操作人员技术水平有限，在网络系统维护阶段也可能产生安全漏洞。尽管某些系统提供了安全机制，但由于种种原因，这些机制未能充分发挥作用。

3、内部用户的安全威胁

系统内部人员可能因存心攻击、恶作剧或无心之失等原因对网络进行破坏或攻击，这种行为给网络信息系统带来的损失难以预料。移动介质如 U 盘、移动硬盘的交叉使用，以及在连接互联网的电脑上使用，容易导致病毒交叉感染，给校园网络带来较大安全威胁。近年来，利用 ARP 协议漏洞进行的窃听、流量分析、DNS 劫持、资源非授权使用、植入木马病毒等攻击手段不断增加，严重影响了网络安全。

4、软件的漏洞

一般来说，软件的复杂性与漏洞数量成正比。在网络系统运行过程中，由于操作系统自身不够完善，针对系统漏洞的攻击较多且影响严重。目前，办公、下载、视频播放、聊天等软件的广泛使用，使其成为攻击者的目标。

5、病毒的传播

网络的发展使资源共享更加便捷，移动设备的普及也显著提高了资源利用率，但同时也导致病毒泛滥、网络性能急剧下降，许多重要数据因此受到破坏或丢失。网络在提供便利的同时，也成为了病毒传播的重要途径。近年来，病毒的黑客化趋势使得病毒的感染和传播更加快速化、多样化，网络病毒的防范任务愈发严峻。

6、各种非法入侵和攻击

校园网接入点众多，拥有大量公共资源，使用者安全意识淡薄，安全防护薄弱，使其成为易受攻击的目标。非法入侵者有目的地破坏信息的有效性和完整性，窃取数据，非法抢占系统控制权、占用系统资源。常见的攻击手段包括漏洞扫描、口令破解、非授权访问、数据篡改、网络传播病毒或恶意脚本、拒绝服务攻击等。

（二）校园网安全管理和维护的措施与建议

1、配置高性能的防火墙产品

防火墙是设置在不同网络或网络安全域之间的一系列部件组合，通常位于可信赖的内部网络与不可信赖的外部网络之间。它既可以作为分析器，监视或拒绝应用层的通信业务，也可以在网络层和传输层运行，根据预设规则过滤报文分组。通过合理配置防火墙的安全设置，制定恰当的访问控制策略，可以有效保障网络资源不被非法使用和访问。

2、网络设计、使用更合理化

在网络设计初期，应充分考虑终端设备安全事件对网络的影响，明确所需的安全措施。通过身份验证的设备访问网络，防范未经授权的接触，增加入侵者的难度，从而提供可预测、可衡量、有保证的安全服务。

3、软件漏洞修复

在校园网络系统运行过程中，一方面对用户进行分类，划分不同用户等级，规定相应权限；另一方面对资源进行区分，划分不同共享级别，如只读、安全控制、备份等。同时，为不同用户分配独立账户和密码，定期动态修改密码，确保密码有效性；结合防火墙使用，过滤可疑 IP 地址，防止恶意入侵；建立补丁更新服务器，部署全局更新机制，实时高效修复软件漏洞。

4、防杀毒软件系统

在互联网快速发展的当下，病毒种类呈爆发式增长。在校园网中部署带防火墙的企业版杀毒软件，能够有效防护整个校园网络，防止计算机遭受病毒入侵。

5、配备入侵检测系统(IDS)并建立蜜罐陷阱系统

入侵检测通过对计算机网络或系统的关键点信息进行收集和分析，检查是否存在违反安全策略的行为和被攻击迹象。蜜罐系统则通过吸引攻击者并记录其行为，帮助系统及时了解最新攻击手段和漏洞，从而有针对性地防范攻击和修复漏洞。

6、系统安全风险评估

互联网的不安全因素时刻威胁着网络安全。只有对网络系统所面临的风险进行全面有效评估，才能精准掌握存在的漏洞和威胁，进而采取有效措施控制网络风险。风险评估是一个动态循环过程，必须定期、长期开展。

7、制定灾难恢复计划

网络攻击方式和漏洞数量呈逐年上升趋势，管理员难以及时跟上补丁更新步伐，且入侵者往往能在软件厂商修复漏洞之前发现并利用这些漏洞。尤其是缓冲区溢出类型的漏洞，危害性极大且广泛存在，是计算机安全的重大威胁。虽然无法完全防止灾难发生，但通过建立意外事件计划，记录灾难影响并制定相应应对措施，可以将灾难造成的损失降到最低。

8、加强网络安全管理

随着网络技术的飞速发展、应用领域的不断拓展以及用户对网络的深入了解，恶意破坏者或非法入侵者对网络安全的影响日益增大，网络安全管理工作任务愈

发艰巨。因此，必须及时修补漏洞、查看日志，确保网络稳定性。高校应颁布网络行为规范和处罚条例，有效控制和减少来自内部网络的安全隐患。

通过以上措施的实施，可以有效提升高校校园网的安全性，保障校园网的稳定运行，为教育教学和科研活动提供可靠的网络支持。

（三）校园网的安全防范和管理

随着网络技术的广泛普及，人们对网络的依赖程度日益加深。网络破坏所造成的损失和混乱也比以往任何时候都要严重。这使得高校对网络安全的要求不断提高，网络安全的重要性也日益凸显，其发展与网络应用的演进密切相关。

在国家网络信息化建设飞速发展的背景下，越来越多的学校建立了自己的校园网络，用于教学和管理。通过 Internet 的远程教育网络，教育不再受国家、地区、学校、学科的限制，学生能够充分享受教育的多样性，提升学习的趣味性和选择性。然而，与此同时，黑客攻击事件愈演愈烈，非法信息蔓延，网络病毒爆发，邮件蠕虫扩散，这些都给校园网蒙上了阴影。校园网及远程教育网络系统中同样存在诸多威胁网络安全的因素。

以益阳职业中专学校为例，其校园网的安全隐患和威胁主要来自病毒和黑客入侵，但防护重点有其特定需求。校园网需要加强安全防范和管理的三个方面如下：

（1）防范病毒入侵

当前，网络中的病毒种类繁多且不断更新。以红色代码、Nimda、SQL Slammer 等病毒为例，它们已经成为集蠕虫、病毒和黑客工具于一体的复合型威胁。这些病毒利用邮件这一最广泛的应用手段，随时准备破坏数据、瘫痪网络。

（2）监控网络流量

Internet 的开放性使得网络信息复杂多样。学生可以轻松访问和浏览各类网站，包括色情、暴力及游戏等不良内容。各种非法和有害信息，如色情、暴力内容，甚至邪教的歪理邪说等，通过 Internet 涌入校园，对未成年学生群体造成不良诱导，可能在其心灵深处留下负面影响。

（3）保护关键资源

教学资料、考试试题、学生档案、招生信息等重要数据是校园网中最为宝贵

的关键资源，也是非法入侵者的主要攻击目标。例如，2002 年一位教师因个人不满侵入学校服务器，篡改并破坏了许多学生成绩档案，给学校和教育部门带来了巨大损失。此外，一旦病毒爆发，这些数据也面临被破坏或丢失的风险。

网关防护：筑牢第一道防线

网关是校园网络连接到 Internet 的出入口，也是大多数病毒和入侵行为的必经之地。网关防护如同学校的大门，把好这第一道关，可以极大地减轻校园网内部的安全防范压力，实现事半功倍的效果。

三 、益阳职业中专学校园网安全隐患解决方案与实现

（一）防火墙的选择与设计

防火墙作为网络防护的首要防线，其重要性已被广泛认可。为了满足益阳职业中专学校园网的安全需求，我们对防火墙的性能和管理特点进行了全面评测。在本次评测中，共有 AXENT、Check Point、Cisco、Cyber Guard、NetGuard、NetScreen 和 Secure Computing 七家厂商的产品参与。评测维度涵盖了防御功能、应用层高级代理功能、网络地址转换支持、认证支持、协议支持、加密支持以及 LAN 接口等多个方面。经过综合评估，Cisco 的 PIX 防火墙凭借其接近线速的高性能，脱颖而出，被认为是最符合学校网络安全需求的产品。益阳职业中专学校防火墙网络拓扑图如图 3.1。

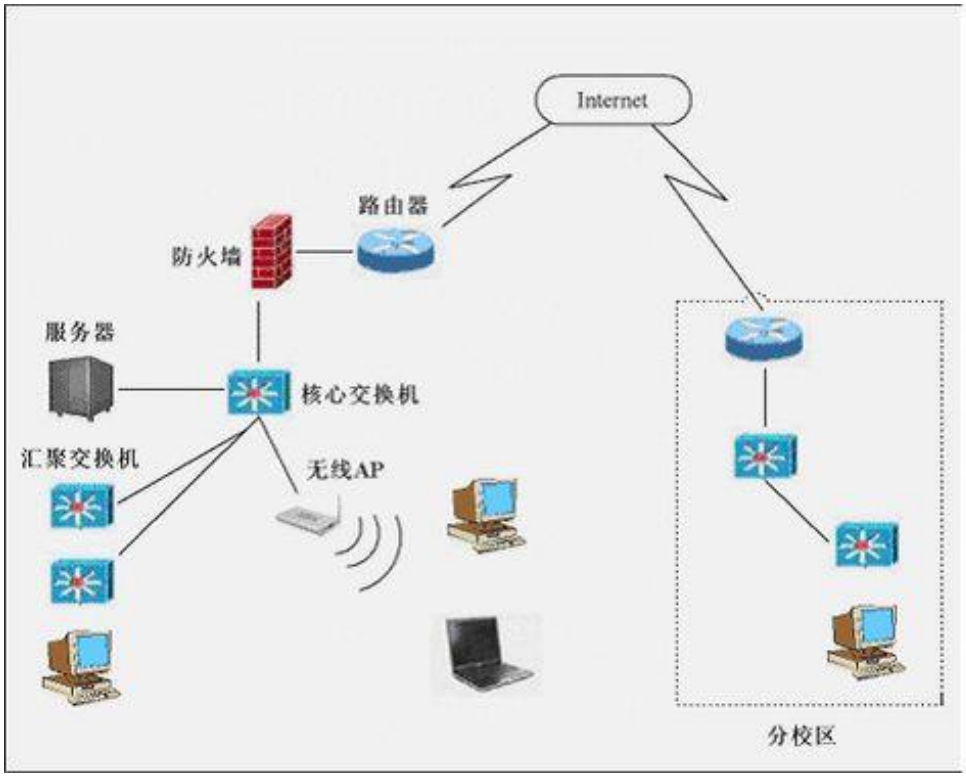


图 3.1　益阳职业中专学校防火墙网络拓扑图

1、Cisco PIX525 防火墙

Cisco PIX525 防火墙是网络间的关键防护设备，能够有效防止非法入侵并过滤信息。从结构上看，它类似于一台工业级计算机主机，配备闪存（Flash）

和专用的防火墙操作系统。其硬件设计与工控机相似，适合 24 小时不间断运行。外观上，它与路由器类似，采用机架式标准设计，高度为 2U。正面仅有一些指示灯，而背面则配备了两个以太网口（RJ-45）、一个配置口（console）、两个 USB 接口、一个 15 针的 Failover 口以及三个 PCI 扩展口。

2、 Cisco PIX525 防火墙的安装和配置

(1)硬件安装

将 PIX 防火墙安装到机架中，检查电源系统后连接电源并开机。确保所有硬件连接稳固，以保障设备的稳定运行。

(2)初始配置

使用配置线将计算机的 COM2 口连接到 PIX525 的 console 口。通过 Windows 系统中的“超级终端”软件进行连接，保持默认的通信参数设置。初次使用时，需要完成初始化设置，包括以下内容：

日期（Date）：设置系统日期。

时间（Time）：设置系统时间。

机名（Hostname）：设置防火墙的主机名称。

内部 IP 地址（Inside IP Address）：配置内部网卡的 IP 地址。

域名（Domain）：设置主域名。

完成上述设置后，系统将保存配置，完成初始化过程。此后，通过超级用户模式（enable）登录，初始密码为空。为了保障系统安全，建议立即使用 passwd 命令修改默认密码。

(3)激活以太端口

激活以太端口必须用 enable 进入，然后 configure 模式

PIX525>enable　　// 进入特权模式，需要输入密码

Password:

PIX525#config t　　// 进入全局配置模式，用于进行系统配置

PIX525(config)#interface ethernet0 auto　　// 将接口 ethernet0 的工作模式设置为自动协商，以适应连接的设备

PIX525(config)#interface ethernet1 auto　// 将接口 ethernet1 的工作模式设置为自动协商，以适应连接的设备

在默然情况下 ethernet0 是属外部网卡 outside, ethernet1 是属内部网卡 inside。inside 在初始化配置成功的情况下已经被激活生效了，但是 outside 必须命令配置激活。

(4)命名端口与安全级别

采用命令 nameif

PIX525(config)#nameif ethernet0 outside security0　// 将接口 ethernet0 命名为 "outside"，并设置其安全级别为 0

PIX525(config)#nameif ethernet0 outside security100　// 这条命令是重复的，应该是误输入。正确的命令应该是针对另一个接口

security0 是外部端口 outside 的安全级别（100 安全级别最高）

security100 是内部端口 inside 的安全级别,如果中间还有以太口，则 security10，security20 等等命名，多个网卡组成多个网络，一般情况下增加一个以太端口作为 DMZ(Demilitarized Zones 非武装区域) [7]。

(5)配置以太端口 IP 地址

采用命令为：ip address

内部网络为：192.168.1.0 255.255.255.0

外部网络为：222.20.16.0 255.255.255.0

PIX525(config)#ip address inside 192.168.1.1 255.255.255.0　// 为 "inside" 接口（内部网络接口）配置 IP 地址 192.168.1.1

PIX525(config)#ip address outside 222.20.16.1 255.255.255.0　// 为 "outside" 接口（外部网络接口）配置 IP 地址 222.20.16.1

(6)配置远程访问（telnet）

PIX 的以太端口是不允许 telnet 的，这一点与路由器有区别。Inside 端口可以做 telnet 就能用了,但 outside 端口还跟一些安全配置有关。

PIX525(config)#telnet 192.168.1.1 255.255.255.0 inside　// 允许从内部网络（192.168.1.0/24）通过 Telnet 访问防火墙的内部接口 IP 地址 192.168.1.1

PIX525(config)#telnet 222.20.16.1 255.255.255.0 outside // 允许从外部网络（222.20.16.0/24）通过 Telnet 访问防火墙的外部接口 IP 地址 222.20.16.1

测试 telnet

在[开始]->[运行]

telnet 192.168.1.1

PIX passwd：

输入密码：cisco

(7)访问列表（access-list）

有 permit 和 deny 两个功能，网络协议一般有 IP、TCP、UDP、ICMP 等等，只允许访问主机:222.20.16.254 的 www,端口为：80

PIX525(config)#access-list 100 permit ip any host 222.20.16.254 eq www // 创建访问控制列表（ACL）100，允许任何 IP 地址访问外部网络中的主机 222.20.16.254 的 HTTP（www）服务

PIX525(config)#access-list 100 deny ip any any // 在访问控制列表 100 中添加一条规则，拒绝任何 IP 地址之间的任何 IP 流量，作为默认拒绝规则

PIX525(config)#access-group 100 in interface outside // 将访问控制列表 100 应用于外部接口（outside），方向为入站流量

(8)地址转换（NAT）和端口转换（PAT）

首先必须定义 IP Pool，提供给内部 IP 地址转换的地址段，接着定义内部网段。

PIX525(config)#global (outside) 1 222.20.16.100-222.20.16.200 netmask 255.255.255.0 // 定义全局地址池，用于 NAT 转换。将外部接口（outside）的 IP 地址范围 222.20.16.100 到 222.20.16.200 分配给全局地址池 1，子网掩码为 255.255.255.0

PIX525(config)#nat (outside) 1 192.168.0.0 255.255.255.0 // 配置 NAT 规则，将内部网络 192.168.0.0/24 的流量转换为全局地址池 1 中的地址

如果是内部全部地址都可以转换出去则：

PIX525(config)#nat (outside) 1 0.0.0.0 0.0.0.0 // 配置默认的 NAT 规则，将所有流量转换为全局地址池 1 中的地址

外部地址是很有限的，有些主机必须单独占用一个 IP 地址，必须解决的是公用一个外部 IP(222.20.16.201),则必须多配置一条命令，这种称为（PAT），这样就能解决更多用户同时共享一个 IP,有点像代理服务器一样的功能。配置如下：

PIX525(config)#global (outside) 1 222.20.16.100-222.20.16.200 netmask 255.255.255.0 // 定义全局地址池 1，用于 NAT 转换。将外部接口（outside）的 IP 地址 222.20.16.201 分配给全局地址池 1，子网掩码为 255.255.255.0

PIX525(config)#global (outside) 1 222.20.16.201 netmask 255.255.255.0 // 定义全局地址池 1，用于 NAT 转换。将外部接口（outside）的 IP 地址 222.20.16.201 分配给全局地址池 1，子网掩码为 255.255.255.0

PIX525(config)#nat (outside) 1 0.0.0.0 0.0.0.0 // 配置默认的 NAT 规则，将所有流量转换为全局地址池 1 中的地址。这通常用于将内部网络的流量转换为外部 IP 地址。

(9)DHCP Server

在内部网络，为了维护的集中管理和充分利用有限 IP 地址，都会启用动态主机分配 IP 地址服务器，下面简单配置。

地址段为 192.168.1.100—192.168.168.1.200

DNS: 主 202.96.128.68 备 202.96.144.47

主域名称：abc.com.cn

DHCP Client 通过 PIX Firewall

PIX525(config)#ip address dhcp // 配置防火墙的接口通过 DHCP 获取 IP 地址。这通常用于动态分配 IP 地址，适用于需要频繁更改 IP 地址的环境

DHCP Server 配置：

PIX525(config)#dhcpd address 192.168.1.100-192.168.1.200

inside

PIX525(config)#dhcp dns 202.96.128.68 202.96.144.47 // 配置 DHCP 服务器为客户端分配 DNS 服务器地址。这里指定的两个 DNS 服务器地址分别为 202.96.128.68 和 202.96.144.47

PIX525(config)#dhcp domain abc.com.cn // 配置 DHCP 服务器为客户端分配默认的域名后缀，这里指定的域名后缀为 abc.com.cn

(10)静态端口重定向

PIX525 增加了端口重定向的功能，允许外部用户通过一个特殊的 IP 地址端口通过 Firewall PIX525 传输到内部指定的内部服务器。这种功能也就是可以发布内部 WWW、FTP、Mail 等服务器了，这种方式并不是直接连接，而是通过端口重定向，使得内部服务器很安全[9]。

命令格式：

static

[(internal_if_name,external_if_name)]{global_ip|interface}

local_ip

[netmask mask][max_cons[max_cons[emb_limit[norandomseq]]]

static

[(internal_if_name,external_if_name)]{tcp|udp}{global_ip|interface}

local_ip

[netmask mask][max_cons[max_cons[emb_limit[norandomseq]]]

外部用户直接访问地址 222.20.16.99

telnet 端口，通过 PIX 重定向到内部主机 192.168.1.99 的 telnet 端口（23）。

PIX525(config)#static (inside,outside) tcp 222.20.16.99

telnet 192.168.1.99 telnet netmask 255.255.255.0

外部用户直接访问地址 222.20.16.99

FTP，通过 PIX 重定向到内部 192.168.1.3 的 FTP Server。

PIX525(config)#static (inside,outside) tcp 222.20.16.99

ftp 192.168.1.3 ftp netmask 255.255.255.0

外部用户直接访问地址 222.20.16.208

www(80 端口)，通过 PIX 重定向到内部 192.168.123 的主机的 www(80 端口)。

PIX525(config)#static (inside,outside) tcp 222.20.16.208

www 192.168.1.2 www netmask 255.255.255.255 0 0

外部用户直接访问地址 222.20.16.201

HTTP(8080 端口)，通过 PIX 重定向到内部 192.168.1.4 的主机的 www(即 80 端口)。

PIX525(config)#static (inside,outside) tcp 222.20.16.208

8080 192.168.1.4 www netmask 255.255.255.0

外部用户直接访问地址 222.20.16.5

smtp(25 端口)，通过 PIX 重定向到内部 192.168.1.5 的邮件主机的 smtp(即 25 端口)

PIX525(config)#static (inside,outside) tcp 222.20.16.208

smtp 192.168.1.4 smtp netmask 255.255.255.0

(11)显示与保存结果

采用命令 show config

保存采用 write memory[2]

（二）校园网身份认证系统的选择与设计

在校园网建设过程中，多个应用系统通常在不同时间开发完成。由于各应用系统在功能、设计方法和开发技术上存在差异，形成了各自独立的用户库和认证体系。随着校园网的发展，用户群体逐渐扩大，一个用户可能使用多个应用系统，但每个系统都有独立的账号。这种分散的认证方式给用户带来了不便，用户希望在登录校园网后，无需再次认证即可直接进入各个应用系统。这种需求被称为“单点登录”。

1、需求分析

在多个独立用户体系的应用系统中实现单点登录，需要考虑以下关键问题：

基于 B/S 模式：单点登录系统的实现需基于各应用系统均采用浏览器/服务器（B/S）模式的前提。

统一用户认证标志：用户登录后应获得一个统一的用户令牌，该令牌需被各应用系统认可。

安全加密与时效性：用户令牌必须是安全加密的，并且应设定有限的时效期，以确保安全性。

统一用户账号：由于用户在不同应用系统中可能使用不同的账号，因此需要为每个用户设置一个统一的账号，用于单点登录。该统一账号需与用户在各应用系统中的账号建立映射关系。

跨域支持：各应用系统可能属于不同的网络域，因此单点登录系统需要支持跨域认证。

系统改造与开发：已上线的应用系统需要进行改造以支持单点登录，而正在开发的应用系统应在开发阶段增加对单点登录的支持。同时，各应用系统之间应保持松耦合关系。

最小化对现有认证体系的冲击：由于各应用系统已处于稳定运行期，单点登录系统的实现应尽量减少对现有登录认证体系的影响，确保原有登录流程依然可用。

尽管一些应用服务器平台提供了对单点登录的支持，但它们通常要求应用系统的用户认证设计符合特定规范。对于已经稳定运行的应用系统来说，这种要求难以实现，因此需要寻找一种更为灵活的解决方案，以最小化对现有系统的改造成本和风险。

通过以上分析，我们可以明确单点登录系统的设计目标：在不影响现有应用系统稳定性的前提下，实现用户在校园网中的便捷登录和跨系统访问，提升用户体验，同时确保系统的安全性。

2、设计

系统的整体设计结构如图 3.2。

图 3.2 系统结构

3、单点登陆的设计流程

单点登录系统的设计包括登录和登出两个主要部分。以下是登录流程的详细设计：

登入流程：

单点登录的登录流程如下：

（1）用户通过 URL 发起对子系统的访问请求。

（2）子系统根据用户传入的 URL，判断 URL 中是否存在 State 参数。

（3）如果存在 State 参数，直接跳转到步骤（4）。如果不存在 State 参数，说明用户是首次登录该系统，子系统将跳转到 SSO（单点登录）服务器进行用户验证，并将当前页面的 URL 作为参数传递给 SSO 系统。

（4）SSO 服务器根据传入的 URL，判断 URL 中是否存在用户名和密码参数。如果存在用户名和密码参数，SSO 服务器将验证用户名和密码的正确性，并根据验证结果设置 State 状态值。

如果验证通过，设置 State 状态值为 4（合法用户）。

如果验证失败，设置 State 状态值为 1（非法用户）。

验证完成后，SSO 服务器将状态值返回给子系统，并跳转到步骤（1）。

（5）如果 URL 中不存在用户名和密码参数，SSO 服务器将读取客户端本地的 Cookie 信息：

如果客户端不存在 Cookie，说明用户是首次访问系统，SSO 服务器将设置 State 状态值为 1（未登录用户），并将状态值返回给子系统，跳转到步骤（1）。

如果客户端存在 Cookie，SSO 服务器将读取 Cookie 信息，判断该用户是否为合法登录用户，并根据结果设置 State 状态值。

如果用户具有使用权限，设置 State 状态值为 2（已登录用户）。

如果用户没有使用权限，设置 State 状态值为 3（无权限用户）。

SSO 服务器将状态值返回给子系统，并跳转到步骤（1）。

（6）子系统根据 State 状态值进行相应的跳转：

如果 State 状态值为 2 或 4，说明用户已通过验证，子系统将跳转至相应的服务页面。

如果 State 状态值为 1 或 3，说明用户未通过验证或无权限，子系统将跳转到登录页面，提示用户重新登录。

优化后的文字表达：

单点登录的设计涵盖了登录与登出两大环节。以下是登录流程的详细阐述：

登录流程：

用户通过 URL 向子系统发起访问请求。

子系统检查 URL 中是否包含 State 参数。

若存在 State 参数，直接进入下一步；若不存在，表明用户首次登录该子系统，子系统将请求转发至 SSO 服务器进行用户身份验证，并附带当前页面 URL 作为参数。

SSO 服务器接收 URL 后，检查其中是否含有用户名和密码信息：

若存在用户名和密码，SSO 服务器将对这些凭证进行验证。验证通过则设置 State 状态值为 4（表示合法用户），验证失败则设置为 1（表示非法用户），随后将状态值反馈给子系统，并返回第一步。

若 URL 中未包含用户名和密码，SSO 服务器将尝试读取客户端本地的 Cookie。

若 Cookie 不存在，认定用户首次访问系统，设置 State 状态值为 1（未登录用户），并将状态值反馈给子系统，返回第一步。

若 Cookie 存在，SSO 服务器将读取并验证用户身份。若用户具备相应权限，设置 State 状态值为 2（已登录用户）；若无权限，设置为 3（无权限用户）。之后将状态值反馈给子系统，返回第一步。

子系统依据 State 状态值进行页面跳转：

若 State 状态值为 2 或 4，表明用户已通过身份验证，子系统将直接跳转至对应的服务页面。

若 State 状态值为 1 或 3，表明用户未通过验证或无权限访问，子系统将跳转至登录页面，提示用户重新输入登录信息

根据 state 状态值进行相应的跳转， 如果 state 为 2 或者 4， 跳转至子系统相应的服务页面；如果状态值为 1 或者 3，跳转到登录页面让用户重新登录。单点登入的流程图如图 3.3 所示。

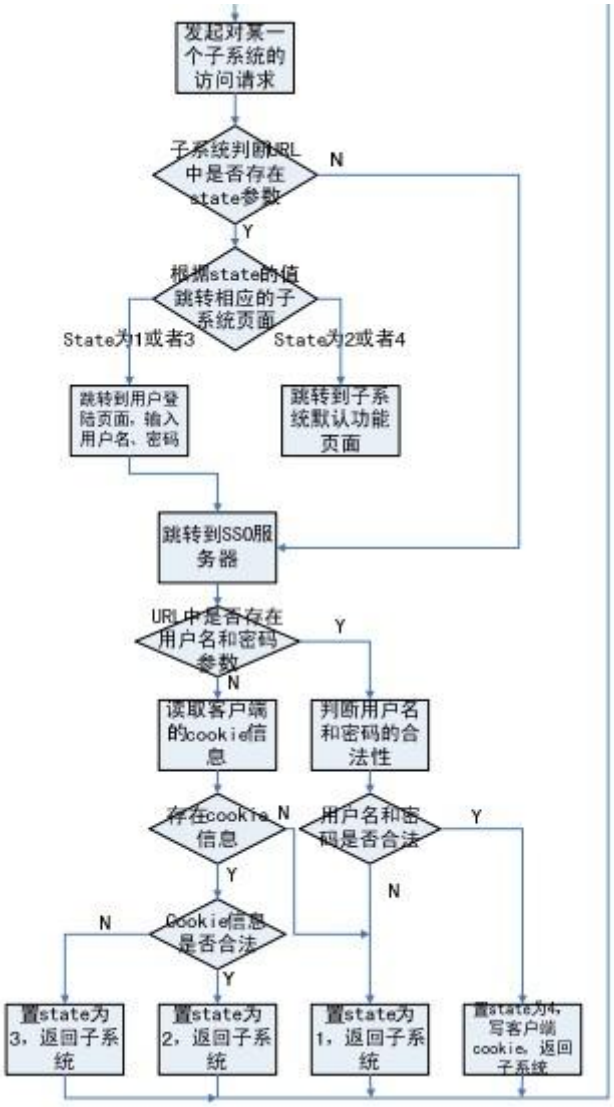


图 3.3　单点登入流程图

为了确保系统的安全性，我们仅在 Cookie 中记录用户的用户名和 IP 地址，并对这些信息进行加密处理。当用户首次登录时，SSO 服务器会将用户的用户名及其当前 IP 地址写入 Cookie。当用户再次请求其他系统的服务时，SSO 服务器会验证 Cookie 中的信息，判断其中的用户名和 IP 地址是否与当前请求服务的用户信息一致。如果一致，表明用户已登录，可直接使用请求的服务；如果不一致或 Cookie 不存在，则需用户重新登录。通过加入 IP 信息，我们有效防止了 Cookie 被复制到其他机器上使用的情况。此外，SSO 服务器对用户进行 Cookie 操作，解决了不同站点之间的跨域问题。

登出流程：

用户使用系统完毕后，需安全退出登录，确保后续用户无法利用前一用户的登录信息进行登录。登出流程如下：

（1）客户端发起登出请求；

（2）子系统将登出请求重定向至 SSO 的登出页面；

（3）SSO 服务器删除客户端的 Cookie；

（4）删除客户端 Cookie 后，跳转至子系统的登出页面；

（5）退出所有系统。

单点登录系统的安全性：

单点登录系统的安全性至关重要。本系统采用多种机制确保子系统与 SSO 系统之间通信的安全性。对于 SSO 服务器与子系统传递的信息，我们采用非对称加密和数字签名的方式，保障数据的真实性与完整性。针对客户端的 Cookie，我们采用内存 Cookie，记录用户 IP 等信息并进行加密，确保 Cookie 的安全性。

cookie 的安全性保证：

在登录过程中，SSO 服务器通过读取客户端 Cookie 信息来判断用户是否已登录。为确保 Cookie 的安全性，我们仅记录用户的用户名和 IP 地址，不存储密码信息，并对这些数据进行加密处理。同时，我们采用内存 Cookie，仅保存在内存中，用户关闭浏览器后 Cookie 自动失效，防止非法用户盗取合法用户的 Cookie。

服务器与站点之间信息传输的安全保证：

在登录流程中，子系统与 SSO 服务器之间需通过 URL 跳转传递状态信息、用户名和密码。为确保这些信息的安全性，我们采取以下措施：

（1）首次访问子系统：子系统生成一个随机值作为登录 ID，构造包含子系统 ID、登录 ID、返回子系统的 URL 和数字签名的 URL，重定向至 SSO 服务器。数字签名通过对“登录 ID + 返回 URL”进行 MD5 哈希后再用 RSA 公钥加密生成。SSO 服务器收到请求后，用 RSA 私钥验证签名，验证通过后继续后续流程。

（2）子系统登录页面提交：用户在子系统登录页面输入用户名和密码并提交后，子系统将用户名和密码用 RSA 公钥加密，并生成包含子系统 ID、登

录 ID、加密后的用户名和密码、返回 URL 和数字签名的 URL，跳转至 SSO 服务器。数字签名通过对“用户名 + 密码 + 登录 ID + 返回 URL”进行哈希后再用 RSA 公钥加密生成。SSO 服务器收到请求后，验证签名并解密用户名和密码，核对用户合法性。

（3）从 SSO 服务器返回子系统：SSO 服务器返回子系统时，构造包含状态、登录 ID 和数字签名的 URL。子系统首先验证数字签名，验证通过后进行相应逻辑处理。同样，在用户登出时，也需经过签名验证。

通过数字签名，即使数据被截获，篡改后的信息也无法通过验证，从而确保数据的真实性。此外，我们还可采用 SSL 传输机制，进一步提升系统的安全性。

（三） Chost 数据备份实现

1、数据智能备份设计

数据智能备份系统主要由具备自动加载功能的磁带库硬件产品和具备数据库在线备份功能的自动备份软件组成。该系统能够实现自动备份管理，具备数据备份系统的分布处理、集中管理、备份机器分组管理、备份介质分组管理、备份数据分类分组管理以及备份介质自动重复使用等多项功能。备份数据可以在每个备份客户机上按需恢复，也可以在同一平台上根据用户权限进行交叉恢复。数据备份操作可以采用集中自动执行或手动执行的方式。

（1）实现系统的灾难恢复

数据智能备份系统能够确保在发生灾难时，系统可以快速恢复，减少数据丢失和业务中断的风险。

（2）对应用系统无不良影响

备份系统的设计应确保不会对应用系统的性能和稳定性产生任何负面影响，保证业务的连续性。

（3）系统扩展能力

备份系统的设计应考虑未来的扩展需求，提供平滑升级的能力，以适应业务增长和技术发展的需要。

2、数据备份设计硬件

目前，数据备份主要依赖手工操作，需要投入大量人力，并且容易因人为错误而导致故障。手工备份存在以下问题：

需要频繁更换磁带，备份的准确性和完整性难以保证。

操作复杂，速度慢，影响系统的总体效率和自动化水平。

操作人员需要耗费大量时间进行备份操作。

磁带仅用于存放数据，难以实现归档、异地存放及规范化管理。

故障备份难以被及时发现，可能导致数据丢失和失效。

为保障业务数据的安全，应利用自动控制装置加强对磁带的集中备份管理。目前，数据智能备份系统的存储硬件通常选用自动磁带库。自动磁带库是一个封闭的机箱，集成了 1 台或多台磁带机以及一定数量的磁带，通过机械手臂实现自动装填磁带的功能。其操作是自动完成的，无需人为干涉。磁带库的大容量和连续备份能力，以及自动搜索磁带和自动换带的功能，是单台或多台磁带机无法比拟的。特别是与备份管理软件配合时，能够实现许多自动化功能。磁带库内部的良好环境可以有效保护磁带机和磁带，延长其使用寿命。

3、数据备份设计软件

数据备份软件供应商推出了多种集中备份软件，这些产品都采用了集中机制，通过专用的备份服务器和直接连接的存储设备进行数据备份。一个集中数据备份系统的设计涉及多个不同的软件和硬件模块。数据备份设计软件需要具备以下功能：

（1）集中管理

中央或主服务器负责控制整个数据备份环境，包括索引、备份调度、客户群组定义和硬件配置。主服务器还负责记录备份中的问题，并向系统管理员报告这些问题。

（2）介质服务器管理

数据备份软件应能管理介质服务器，通常通过光纤通道或并行 SCSI 将介质服务器连接到磁带设备上进行数据备份。

（3）客户端自我备份

数据备份客户端是备份软件的重要组成部分，安装在每个需要备份服务的系统中，包括主服务器和介质服务器。客户端软件可以对自己进行备份。

（4）数据安全性与恢复性

备份软件应确保服务器系统及关键业务数据（如数据库数据）的可管理性、高安全性、完整性及易恢复性。

（5）平台支持

备份软件应能很好地支持 Windows 2016 平台系统的应用环境。

（6）无人值守备份

在满足性能的前提下，备份软件应支持无人值守在线备份，易于实施和管理。

（7）快速恢复

在发生数据灾难时，备份软件应能快速、有效地恢复备份数据。

4、数据备份软件的安装与实现

微软公司、IBM、HP、戴尔等国际大公司一致推荐使用的 Veritas 公司的 Backup Exec 9.0 是一款优秀的备份和恢复产品。以下是 Backup Exec 9.0 的安装实现过程：

（1）安装 Backup Exec 9.0

打开 Backup Exec 9.0 安装程序。

按照安装向导的提示进行操作，完成软件的安装。

在安装过程中，选择将主模块安装在运行 Windows 2016 的服务器上。

（2）安装 SQL 和灾难恢复选件

在备份服务器上安装 SQL 和灾难恢复选件。

安装完成后，即可对网络上的 SQL 服务器进行数据备份，并对各台服务器进行灾难恢复操作。

（3）使用 Norton Ghost 2016 进行系统备份

Norton Ghost 2016 是 Symantec 公司生产的免费数据备份与恢复工具，适用于 Windows 操作系统的备份与恢复。以下是其具体安装实现过程：

打开 Norton Ghost 2016 主界面。

运行备份向导：点击“Ghost 基本功能”中的“备份”选项，启动备份向导。

选择源磁盘分区：点击“下一步”，选择要备份的源磁盘分区（如 C 盘），并选择文件（F）。

选择备份文件存储位置：点击“下一步”，指定备份文件的存储位置。

进入高级设置：点击“下一步”，进入“高级设置”界面，点击“高级设置”。

配置高级选项：分别对“外部存储”“压缩”“映像密码”进行设置。

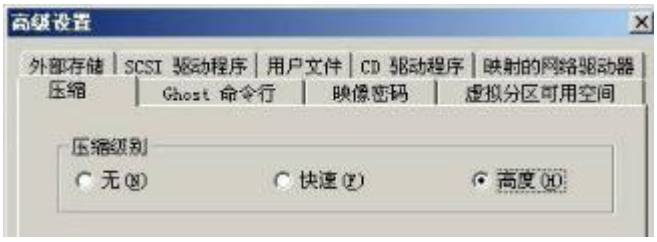


图 3.4 压缩级别

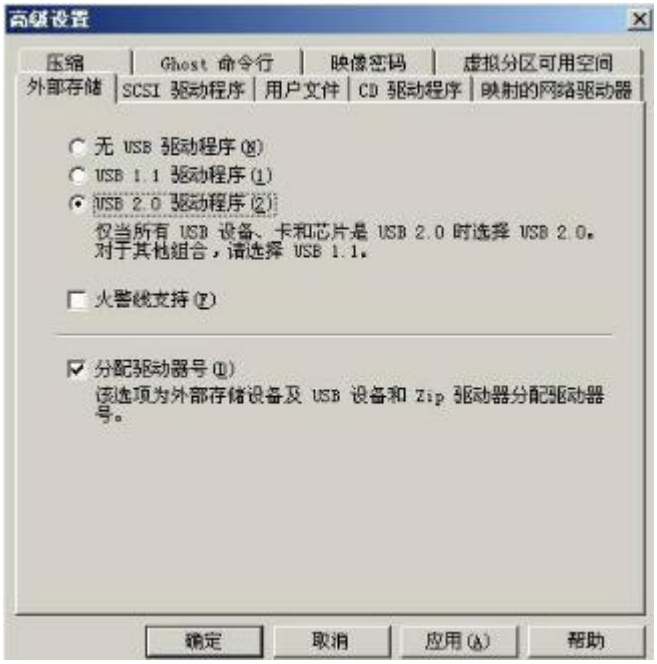


图 3.5 外部存储

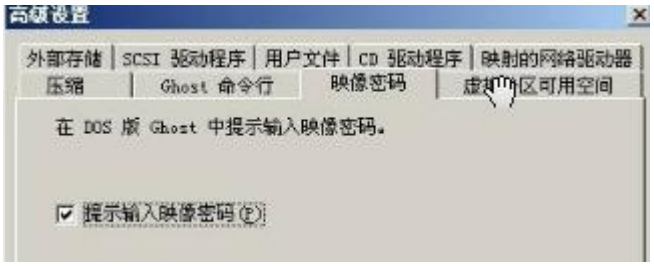


图 3.6 映像密码

7.应用设置并执行备份：应用设置后，点击“下一步”，点击“立即运行”，并在弹出的对话框中点击“确定”。系统将自动重启，并进入 Chost 模式，生成映像文件。

图 3.7 备份向导

（四）入侵检测系统的实现

1、金诺入侵检测系统的组成

网络传感器是金诺入侵检测系统的核心组件之一，用于监控网络流量并检测潜在的安全威胁。以下是网络传感器的主要接口及其功能：

管理口：需分配 IP 地址，用于系统管理和配置。IP 地址需在控制台软件中进行设置。

监听口：与交换机上的监听端口相连，用于捕获网络流量。该接口不分配 IP 地址。

USB 接口：在系统启动前，需插入已设置好的 USB 配置盘，以便加载系统配置和授权信息。

光驱：在系统启动前，需放入 KIDS 的启动光盘，用于引导系统启动。

显示器接口：在系统出现故障时，可连接显示器以查看错误信息。

串口：目前暂不使用。

如图 3.8 所示网络传感器。

图 3.8 金诺入侵检测系统组成

（2）KIDS 引导光盘（Bootable CD）

KIDS 的引导光盘具有以下功能：

用于引导 KIDS 系统启动。

用于安装 KIDS 控制台软件。

（3）KIDS USB 配置盘（Safe Block）

KIDS 的 USB 配置盘具有以下功能：

容量为 16MB。

存储 KIDS 的配置文件，包括网络设置、安全策略等。

存储 License 授权信息，确保系统的合法使用。

（4）控制台软件

控制台软件是用于管理和配置 KIDS 系统的工具，具有以下特点：

可通过 KIDS 的引导光盘进行安装。

推荐在 Windows 2016 操作系统上运行。

传感器的安装：

a.将传感器安装到机架上，并连接好电源。

b.使用网线或光纤将传感器的监听口连接到交换机的镜像端口。

c.使用网线将传感器的管理口连接到交换机的某个端口。

2、控制台软件的配置

（1）控制台安装要求

1) 支持Windows 2016操作系统。
2) CPU：最低PII 350。
3) 内存：最低128M。
4) 硬盘：最低200M剩余空间，建议20G剩余空间。
5) 网卡：PCI 10M/100M网卡至少一块。
6) USB接口：USB 1.1。
7) 显示器、键盘、鼠标等。
8) 操作系统： Windows2016 Professional/Server/Advanced Server ＋SP2中文版本。

（2）控制台的安装

使用 KIDS 的引导光盘进行安装。

按照安装提示逐步操作。

在安装数据库时，可根据需要选择以下选项。

- ✓ Access数据库
- ✓ 使用远程SQL Server
- ✓ 本地SQL Server
- ✓ 安装MSDE(会占用500M空间）

（3）USB配置盘的设置

为传感器的管理口分配 IP 地址。

为控制台所在的主机分配 IP 地址。

将 USB 配置盘插入控制台主机的 USB 接口。

在控制台菜单中选择“Safeblock 设置”。

初始化 USB 配置盘，并选择 Safeblock 驱动器盘符。

1) 导入License(*.lic文件)。
2) 输入管理口IP、子网掩码、网关。
3) 输入控制台的IP。
4) 最后保存设置。

（4）系统启动

将 KIDS 的引导光盘放入传感器的光驱。

将 KIDS 的 USB 配置盘插入传感器的 USB 接口。

启动传感器的电源。

几分钟后，控制台组件视图中会出现传感器图标，表示系统已成功启动并连接。

3、控制台软件的使用

（1）控制台界面-组件视图3.9。

组件ID	组件地址	应用策略	组件名称
30001	本地	复件 所有事件	事件处理引擎
3	192.168.39.37	复件 所有事件	网络传感器
1	192.168.100.237	复件 所有事件	网络传感器

图标	组件	状态	描述
	事件处理引擎	活动	事件处理引擎正常工作
	事件处理引擎	停止	事件处理引擎已和控制台连接成功，尚未正常工作
	网络传感器	断开	传感器尚未和控制台连接成功
	网络传感器	活动	传感器正常工作
	网络传感器	停止	传感器已和控制台连接成功，尚未正常工作

图 3.9 组件视图及组件状态

（2）设置报警响应参数-如图3.10。

图 3.10 报警响应参数设置

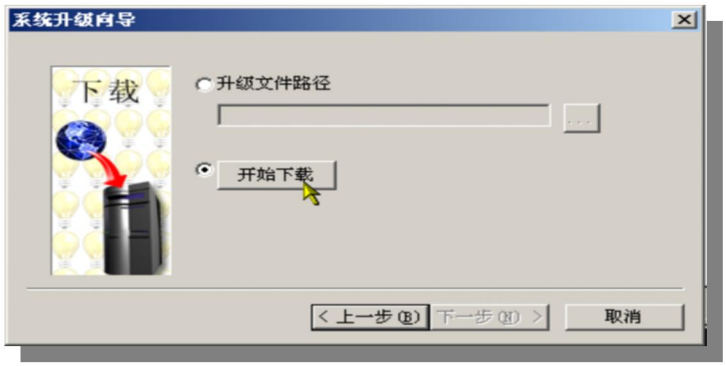
（3）控制台端口扫描设置-如图3.11。

图 3.11 端口扫描设置

（4）控制台参数设置-选项设置图3.12。

图 3.12 选项设置

（5）.系统检测规则的升级-见图3.13，图3.14。



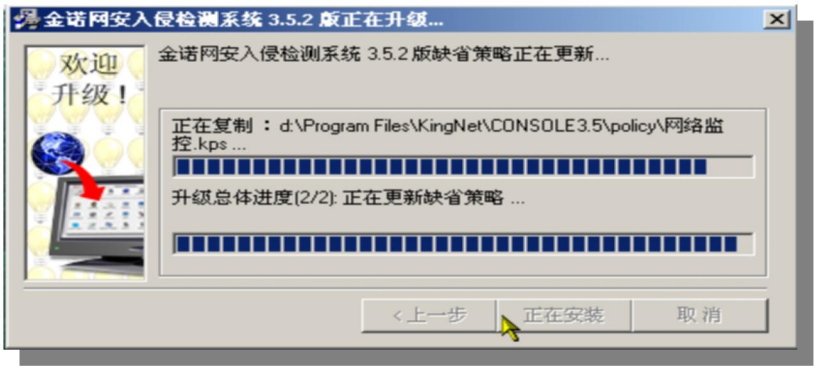


图 3.14 安诺入侵检测系统升级

四、总 结

信息安全与校园安全防御网络的构建与优化:

随着信息化进程的加速，信息安全的重要性日益凸显，逐渐发展成为一个独立的产业。众多技术部门和厂商纷纷推出了新的安全产品，但如何将这些产品有效整合，构建一个协同工作的整体防御体系，通过标准化协议实现相互之间的通信，从而提升整个网络的防御能力，已成为信息安全领域的重要发展方向。这种整合不仅能够充分发挥单一技术或产品的优势，弥补其不足，还能更可靠地保障信息系统的安全运行。

校园安全防御网络的创新架构:

校园安全防御网络作为一种创新的安全架构，其核心优势在于具备自我防御、自我愈合以及集成协同的安全机制。无论是网络系统本身还是网络资源，一旦遭受网络病毒或网络攻击的威胁，该架构能够迅速做出反应，及时发现并阻止攻击行为，同时对病毒或蠕虫进行有效清除，从而显著提升网络安全性能。

网络安全防御系统设计的关键环节:

在网络安全防御系统的设计与实现过程中，本设计主要聚焦于以下几个关键方面：

校园网安全现状的全面调查与分析：深入研究当前校园网面临的主要问题和常见安全隐患，为后续设计提供坚实依据。

基于网络自防御理念的设计策略：探讨安全防御设计策略，构建自防御系统体系架构，以实现网络的自主防护能力。

关键技术研究与部署：深入分析校园网安全隐患及解决方案，研究防火墙与入侵检测技术的原理，基于它们之间的功能互补性进行互动设计，将两者有机结合；详细分析防火墙代理服务器的实现；深入研究 IP Sec 协议，提出动态安全防御系统的设计思路；针对校园网环境下的防病毒系统实现，特别是针对蠕虫特征的防御体系设计；以及针对数据存储安全问题的数据智能备份与恢复方案设计。

系统优化与未来改进方向:

尽管本系统在设计上已取得一定成果，但仍存在诸多可以进一步研究和改进的空间：

互动模型的深化研究：防火墙与入侵检测系统之间的通信协议和语义解释等具体实现细节，以及自身的安全性保护问题，是未来研究的重要方向。

安全防御效果的实验验证：本设计所提出的安全防御系统的实际防御效果，需要在实验环境中进行更深入的验证，以确保其有效性。

网络安全的有机组合：网络安全的实现需要防火墙、VPN、入侵检测、防病毒等技术的互联与互动。这种互动不仅涉及防火墙和入侵检测设备，还应涵盖防火墙与防病毒系统、认证系统之间的关联性，通过这种全面的协同防御机制，才能实现对整个网络的有效保护。

通过以上设计与优化，校园安全防御网络能够更好地应对日益复杂的网络安全挑战，为校园网的安全运行提供坚实的保障。

参考资料

[1] 董袁泉.基于 UML 的高校教材管理系统体系结构建模与实现[D]. 苏州大学，2024.10.

[2]程颐 著·《网络技术与安全》·机械工业出版社·[M]2024.07.

[3]ccitj1·数据备份与灾难恢复·道客巴巴.

[4]万磊 著·《计算机网络工程》·中国铁道出版社·[M]2024.09.

[5]李华·自防御的研究与实现·豆丁.

[6]曹亮 著·《校园网络安全分析及全局网络安全体系设计》·北京工业出版社·[M]2023.02.

[7]myhoo·cisco 防火墙配置·百度百科.

[8]Ramachandran·j 著·《设计安全的体系结构》·北京机械出版社·[M]2022.06.