**课程考核报告**

**（适用于课程论文、提交报告）**

**科 目： 信息安全概论 教 师： 吴开贵**

**姓 名： 谢双骏 学 号： 20194196**

**专 业： 计算机科学与技术 班 级： 1班**

**上课学期： 2022-2023学年第一学期**

**考 生 成 绩：**

|  |  |  |
| --- | --- | --- |
| **卷面成绩** | **平时成绩** | **课程综合成绩** |
|  |  |  |

**阅卷评语：**

**阅卷教师 (签名)**

课程考核要求：

1 以“信息系统安全解决方案”为主题，写一份课程报告。主要论述某类信息系统的概况及所面临的安全威胁，制定详细的安全方案，详述怎样应用安全技术去解决所面临的安全威胁。

题目自拟。例如，“智能园区、智能数据中心、校园网信息系统安全解决方案、大健康行业信息安全解决方案、智能政府、交通、教育、商业、工业互联网信息系统安全解决方案等”。

题目可具体一点，也可以覆盖面稍大一些的行业。例如，细化具体一些的“仓储物流物联网网络安全解决方案”、覆盖面大一些通用性强一些的“工业物联网网络安全解决方案”。

2 论文篇幅不少于8页（不包括封面和目录）

3 每个同学交一份，与其他同学所交论文重复率大于50%，则判定为不及格。

4 报告提交电子版，报告文件命名格式“XX级XX专业X班学号姓名”，例如“22级计科1班20221401001张三”。

目录

[1国内外研究现状 4](#_Toc11735)

[2校园网络问题分析 4](#_Toc13739)

[2.1安全域设计不完善 4](#_Toc22785)

[2.2安全防护系统技术落后 4](#_Toc1659)

[2.3安全制度体系不完善 5](#_Toc8137)

[2.4安全防护系统缺乏整体性 5](#_Toc30237)

[2.5安全防护系统没有主动性 5](#_Toc13846)

[2.6 用户网络安全意识和网络安全技术水平参差不齐 5](#_Toc28736)

[2.7 移动端安全防护系统的忽视 5](#_Toc19124)

[2.7.1校园移动场景的多样性与复杂性 6](#_Toc31468)

[2.7.2校园安全管理与个人隐私的平衡 6](#_Toc23607)

[2.7.3校园业务数据泄露风险高 6](#_Toc4207)

[2.8新冠疫情对安全防护系统的考验 6](#_Toc8624)

[3 高校校园网所受攻击的类型 7](#_Toc418)

[3.1计算机病毒攻击 7](#_Toc3673)

[3.1.1病毒邮件 7](#_Toc27518)

[3.1.2网络病毒 7](#_Toc28520)

[3.1.3基于Web的病毒 7](#_Toc25100)

[3.2间谍软件 7](#_Toc23972)

[3.3假冒网站 7](#_Toc17473)

[3.4垃圾邮件 7](#_Toc18545)

[3.5宽带滥用 8](#_Toc1854)

[3.6Web服务器攻击 8](#_Toc20076)

[3.7网络用户攻击（内部员工） 8](#_Toc32013)

[4安全防护系统设计的理论依据 8](#_Toc30682)

[4.1 WPDRRC模型 8](#_Toc31191)

[4.2满足网络信息安全要素 9](#_Toc18788)

[5 高校校园网解决方案 10](#_Toc5150)

[5.1基本安全防护措施 10](#_Toc6660)

[5.1.1合理的防火墙配置方案 10](#_Toc24455)

[5.1.2核心数据的加密 11](#_Toc11534)

[5.2校园网安全域的设计与划分 12](#_Toc16182)

[5.3 加入网络安全态势感知技术 13](#_Toc22963)

[5.3.1 网络安全态势感知技术的现状 13](#_Toc5070)

[5.3.2 网络安全态势感知技术的架构设计 14](#_Toc4982)

[5.4 基于虚拟安全域技术的移动办公解决方案 16](#_Toc27271)

[5.4.1虚拟安全域 16](#_Toc870)

[5.4.2构建内部移动应用商店 17](#_Toc15878)

[5.4.3防护模块 18](#_Toc8224)

# 1国内外研究现状

随着校园网络建设的加快 , 当前校园网络安全工作越来越重要 , 校园网用户的管理和网络设备的运维逐渐朝着高效化、智能化、精细化的方向发展。随着校园网用户的增多，校园网规模不断扩大，日常运维中常见以下问题：①需要获取用户类型、接入位置、接入方式等信息，以便对网络流量进行设置和优化；②网络设备在运行中出现在线用户不一致问题；③校园网账号开放移动端和 PC 端登录，用户账号存在外借情况；④辅导员老师需要根据学生近期网络使用情况，了解学生的状态；⑤疫情期间，因为云班课和线上教学而陡增的流量压力和分配策略调整。为有效解决上述问题，洪剑珂提出了基于认证系统接口的校园网用户管理系统，孔令峰提出了校园网定时控制互联网访问的方法，李长青等提出了校园网的网络资源精确分配策略。托马斯法维尔等对于新冠肺炎对于校园网的影响做了非常详细的综述。

# 2校园网络问题分析

## 2.1安全域设计不完善

由于经济因素以及对网络安全问题的理解不够前卫，学校现有的业务系统在建设过程中的执行奉信重使用、轻安全的原则，大多数都未按照等级保护要求 , 对不同重要性的业务系统进行区域安全划分，安全设计不合理。同时，即使是在现有的网络信息安全防护体系中仍然存在着大量的信息安全孤岛，不仅这些孤岛无法实现安全防御功能，系统也无法实现整体的安全防御功能。

## 2.2安全防护系统技术落后

随着互联网技术的飞速发展，网络攻击方式也不断地推陈出新，网络攻击事件层出不穷。虽然学校也在网络出口位置配备了入侵检测系统及防火墙 , 实现了一定程度的信息安全保障工作。但防护设备较为陈旧，不足以抵抗现阶段的新型网络安全威胁。传统园区网络采用防火墙和杀毒软件两层安全防御体系。 防火墙通过既定规则在网络层过滤和阻止数据，但不能有效保护 OSI 模型的传输层和应用层。杀毒软件在应用层工作，使用不断更新的病毒数据库和安全规则来保护计算机系统免受攻击，但黑客攻击和特洛伊木马不断出现，如果其病毒数据库不能及时更新，反病毒软件就不能有效地防止新的病毒。在重要网站和信息系统的安全监测、预警和防御方面，也不符合现有的网络安全等级保护的各项技术要求。

## 2.3安全制度体系不完善

学校未根据现有的等级保护要求，从管理制度建立相应的安全防护体系，缺乏完整的安全检查和安全防护制度。同时学校的信息系统种类繁多，又无相关的制度明确相应的管理责任，导致网络安全相关工作人员无法从整体上掌握校内网络安全的整体情况，难于判断可能存在的安全风险，无法推进网络安全工作。

## 2.4安全防护系统缺乏整体性

目前高校校园网存在网络和信息系统的多种安全设备各自为战，无法协同工作、智能联动，以至于不同域的防护系统之间工作都是相互独立的，不能发现和阻止已知、未知威胁，有效整合资源，提高安全事件的检测精度，降低威胁响应时间。大多数校园网都之强调某个安全领域的设备投资，不顾完全保护，很多需要在整体层次上分析的安全漏洞在很长一段时间内仍无法修复。只有整体性攻击等安全风险，快速拦截处置安全事件。

## 2.5安全防护系统没有主动性

目前的大多数高校校园网，基本都是防火墙加杀毒软件的被动防御策略，而想要做到高效的防护，将受到攻击的次数和损失最小化的话，就需要调整防护策略为主动策略。通过汇总、过滤和分析网络安全设备等产生的安全事件，对网络整体上所遭受的安全风险进行多维度评估，分析网络所遭受攻击所处阶段，全面掌握网络整体的安全状况，并能预测出未知网络攻击行为，实现网络安全的主动防御。

## 2.6 用户网络安全意识和网络安全技术水平参差不齐

现今高校校园网的使用人员包括教师，学生，员工等，大多数人的信息安全意识非常淡薄，对于网络攻击可能带来的后果以及如何规避信息安全风险基本上没有任何观念。这往往增加了校园网承受攻击的可能性，同时也增大了网络攻击的波及范围以及造成的损失。用户信息安全意识的提高的价值，有时候甚至远远高于购买更好的设备、做更好的系统所带来的防护价值。

## 2.7 移动端安全防护系统的忽视

随着移动计算时代的到来，我们都经历着从有线到无线的变化，异地办公、远程审批、在线服务、移动学习等高效便捷灵活的移动办公形式，引发了高校科研、管理和服务方式的变革。目前，高校多种业务移动化场景，涉及到多种办公设备和平台。这些应用场景在为教师和学生的校园生活提供了快捷方便的同时，也在一定程度上也带来了安全隐患。

### 2.7.1校园移动场景的多样性与复杂性

相比传统办公，移动办公面临着更加复杂的安全问题，信息数据和计算终端走出高校的安全边界、脱离内部管控、多样的设备类型和复杂的数据运行环境，大大增加了数据泄露的风险。复杂的移动设备系统和类型，不同应用之间的数据交换与共享，面向不同的职能岗位、对象、移动应用的差异化模式管理，权限、对象的复杂化，不同设备数据联通等问题，为高校移动安全管理带来极大挑战。同时，移动化本身涉及到的专业知识与技术架构，与传统的IT环境存在很大差异。

### 2.7.2校园安全管理与个人隐私的平衡

当前师生使用的移动设备上既有个人常用的应用软件，也有工作中需要用到的工作应用：存在个人应用软件可以随意访问、存取工作数据的风险，甚至很容易通过个人应用软件将工作数据非法上传、共享和外泄，工作应用同样也会触及到个人数据。

### 2.7.3校园业务数据泄露风险高

移动设备易丢失、常更换。可以在任何条件下使用，使得每一个移动用户都能够快捷地将工作信息分享、外泄出去，承载了越来越多业务流程及数据的移动设备成为信息泄露的重要风险点

## 2.8新冠疫情对安全防护系统的考验

新冠肺炎大流行导致人们采取了严厉措施来遏制感染的传播。社交距离和封锁措施改变了人们的习惯，而在学校这个范围内，老师和同学对于远程工作、电子教学、在线协作、游戏、视频流媒体的需求陡增，导致校园网内的流量和安全隐患到了一个史无前例的高度。大多数校园网的传入流量急剧下降，而传出流量增加了一倍多，以支持在线学习，远程工作和在线协作也爆发了，高校员工使用协作平台、VPN和远程桌面服务继续在家工作，所有这些突然的变化都给校园网带来了巨大的压力和风险。

2.9 安全防护系统无法可视化

现有的校园网防护系统很难将安全事件以图像或图形的形式呈现给用户，而可视化的界面能够极大的提高管理员处理威胁的效率。

# 3 高校校园网所受攻击的类型

## 3.1计算机病毒攻击

计算机病毒是校园网网络安全的主要威胁， 它可以通过各种形式传播。同时，它的危害也是巨大的。，会影响校园网的传输，瘫痪校园网的运行等。在很多情况下，校园网中的一台计算机会感染病毒，网络中的其他计算机也会感染病毒。

### 3.1.1病毒邮件

源于外部，但是由于内部使用扩散，可能会感染阅读电子邮件的系统，并随后传播到整个组织。

### 3.1.2网络病毒

产生于外部，可能通过不受保护的端口进入，危及整个网络。

### 3.1.3基于Web的病毒

发生在内部对外部的web访问时，可能在浏览时造成危害，进而影响其他内部系统。

## 3.2间谍软件

一些恶意攻击可以利用网络上泛滥的“傻瓜式”间谍攻击软件。不法用户可以在没有任何计算机技术的情况下对校园网进行肆无忌惮的攻击。这对校园网的安全造成了巨大的影响。

## 3.3假冒网站

很多不法分子在网络上设立一些假冒网站，欺骗用户，恶意套取银行账户和密码，给学校师生带来无法弥补的损失。这些钓鱼网站的设置往往与正规网站非常相似，让人难以识别。

## 3.4垃圾邮件

网络上一些人通过大量的垃圾邮件，骗取学校师生的点击率，一方面会使师生使用的电脑感染相关病毒，另一方面也会骗取师生的个人信息，然后非法使用这些个人信息。

## 3.5宽带滥用

BT、迅雷等下载软件在校园网中广泛使用，占用了校园网的带宽资源，使得网络运行缓慢，其他师生无法正常使用。用户在通过下载软件下载网络资源的同时，也存在着将外部网络病毒引入校园网的隐患，对校园网的安全运行产生了很大影响。

## 3.6Web服务器攻击

由外部对Web服务器发起，如果网络服务器被攻破，黑客可以进入网络内部的其他系统。

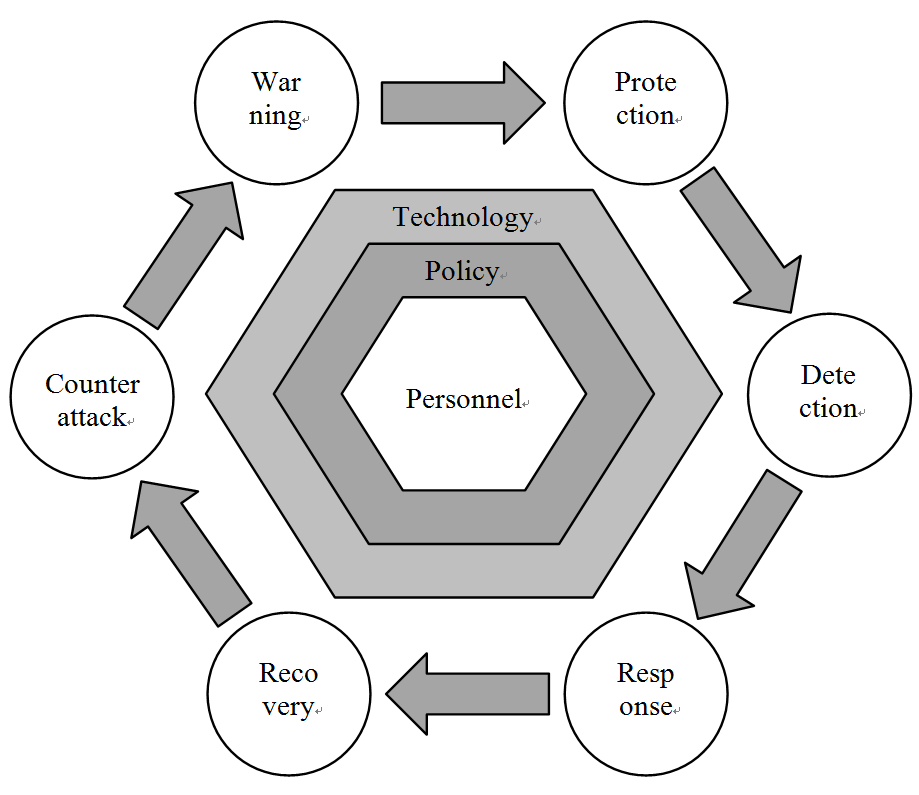
## 3.7网络用户攻击（内部员工）

发生在校园网内部的任何位置，传统的边境防火墙对这种攻击毫无作用，只能用内部分割防火墙来帮助控制损坏。

# 4安全防护系统设计的理论依据

## 4.1 WPDRRC模型

WPDRRC网络信息安全模型是由我国学者在借鉴国外相关模型的基础上，充分结合我国网络信息安全的实际需求而提出的，模型结构如图所示。



它由六个部分组成：

①预警，预测恶意攻击的存在，评估威胁程度，从根本上消除威胁，消除攻击和入侵。

②保护，保护软件、网络和数据安全，确保系统的保密性、完整性、可用性和控制。

③检测，检测系统漏洞和外部威胁，利用漏洞扫描和杀毒软件等手段，实现对网络系统整体安全状况的检测

④响应，依靠每个安全子系统强大的审计、报警、跟踪和处理功能，启动应急响应计划。

⑤恢复，当系统遇到意外事件时，会立即采取一系列措施来恢复系统功能，并尽快提供正常的服务。恢复包括系统恢复和数据恢复。

⑥反击，利用一切手段，保留入侵者的攻击地点和攻击日志作为犯罪证据和线索，必要时使用法律手段对入侵者进行反击。

模型内部的人员，管理和技术是决定安全的因素：

①人是校园网络安全系统中安全因素的核心，在整体信息安全保护中，“人”因素与“技术”因素同样重要。

②管理实际上就是风险控制，其基本过程是对网络管理对象的威胁和漏洞进行分析，确定网络管理对象的价值、网络管理对象发生威胁的可能性、网络管理对象的脆弱性，从而确定网络管理对象的风险等级，再据此选择合适的安全防护措施，降低网络管理对象的风险。

③技术是网络信息安全的保障。要不断适应安全环境的变化，及时更新安全管理策略，积极应用各种新技术、新工具，从不同角度、不同层面进行安全防护，确保网络安全防范体系的良性发展。

设计解决方案的时候一定要考虑上述三个安全因素，然后遵循闭环的流程，系统才会强壮和高效。

## 4.2满足网络信息安全要素

网络信息安全要素有五个方面，分别是：

①可用性：得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。

②可控性：可以控制授权范围内的信息流向及行为方式。

③机密性：确保信息不暴露给未授权的实体或进程。

④完整性：只有得到允许的人才能修改数据，并且能够判别出数据是否已被篡改。

⑤可审查性：对出现的网络安全问题提供调查的依据和手段。

通过上述五个要素，可以得到网络安全的目标：

①使用访问控制机制，阻止“非授权”用户进入网络，即“进不来”，从而保证网络系统的可用性。

②使用授权机制，实现对用户的权限控制，即不该拿走的“拿不走”，同时结合内容审计机制，实现对网络资源及信息的可控性。

③使用加密机制，确保信息不暴露给未授权的实体或进程，即“看不懂”，从而实现信息的保密性。

④使用数据完整性鉴别机制，保证只有得到允许的人才能修改数据，而其他人“改不了”，从而确保信息的完整性。

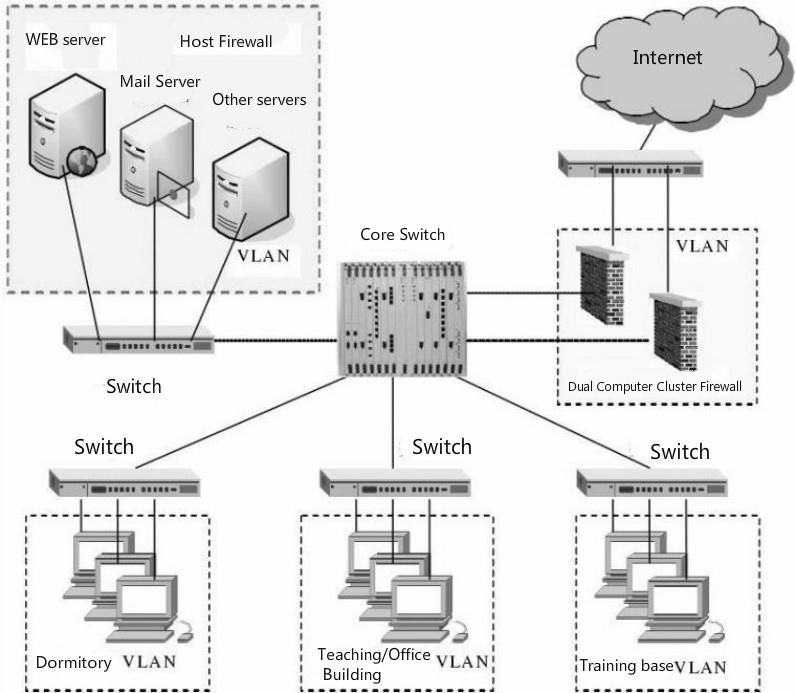
⑤使用审计、监控、防抵赖等安全机制，使得攻击者、破坏者、抵赖者“走不脱”，并进一步对网络出现的安全问题提供调查依据和手段，实现信息安全的可审查性。

# 5 高校校园网解决方案

## 5.1基本安全防护措施

### 5.1.1合理的防火墙配置方案

使用新一代防火墙配置方案，可以解决安全防护系统技术落后的问题，参考Min Huang等人的文章，文中设计了一个改进的校园网防火墙系统方案，如图所示：



其在传统防火墙技术之上有以下提升：

①针对校园网防火墙可能存在单点功能的情况，采用双机集群防火墙的设计，其原理是：如果主防火墙因故障而无效，那么备用防火墙可以及时修复并承担相应的工作。两台防火墙可以方便地进行替换工作，保证了校园网不间断的网络安全防护

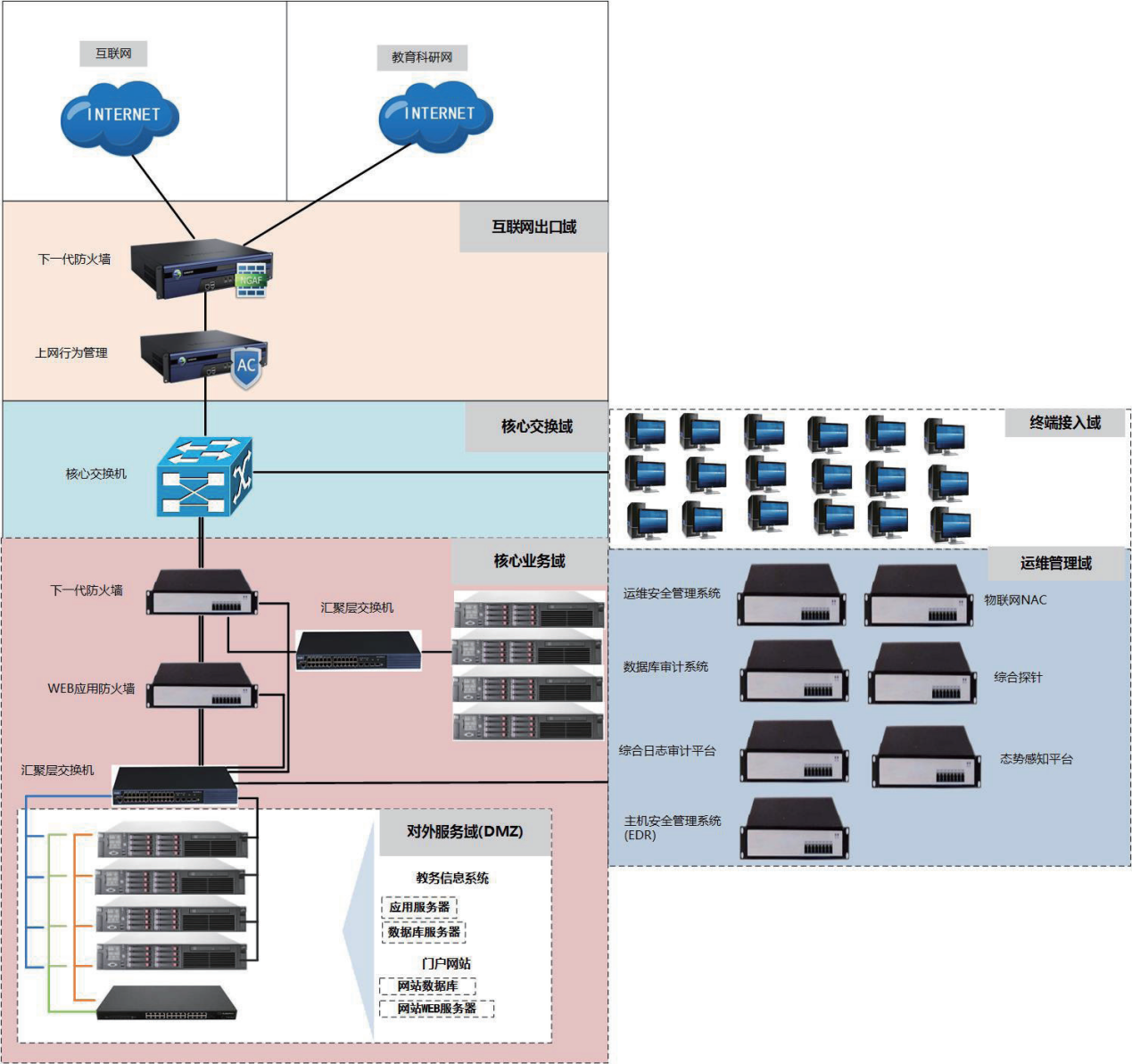
②在内部网络服务器中，根据安全能力的不足，设置了服务器主机防火墙。它的主要职责是拒绝未经授权的访问。服务器主机防火墙是用户感觉不到的。它实现了精确的访问控制，保证了服务器的安全，为校园内部网络服务器全面护航。

### 5.1.2核心数据的加密

校园网中经常发生网络安全事件，如获取、攻击、篡改各类信息，如考试成绩、试卷、学校卡资金信息等。面对这种情况，我们可以采用数据加密的手段，数据加密通常是指改变信息的表达方式，其目的是为了保护真实的信息。这样，未经授权的用户就无法获取受保护的信息。

## 5.2校园网安全域的设计与划分

为了解决安全域设计不完善，安全防护系统去缺乏整体性的问题，将学校的网络拓扑按照等保要求重新规划，分为互联网出口域、核心交换域、对外服务域、核心业务域、运维管理域和终端接入域等区域，并通过在对应区域部署相应的网络安全设备进行防护，安全域划分如图所示：



①互联网出口域：在互联网与内部网络之间部署一台防火墙和上网行为管理系统。出口防火墙开启入侵防御功能和防病毒功能模块，实现对入侵事件的监控、阻断，限制外部网络直接连接到学校的内部网络，保护整体网络各个安全域免受外网常见的恶意攻击。上网行为管理器可以监控校园范围内的上网行为，及时阻止风险操作，规范校园网络秩序

②核心交换域：核心交换域位于互联网出口域和核心业务域之间，负责内网之间各个终端的通信，内网和外网之间的通信，以及设备对核心业务域的通信，主要是由交换机组成。因为该区域到其他部分都有诸如防护墙的安全防护措施，因此在此域中没有必要设置。

③核心业务域：重要的业务系统服务器和数据库是整个系统的核心，如果不和其他内网区域分隔开的话，任何病毒和攻击都可以直达，造成难以承受的损失。因此需要将其单独隔离出来，并在该区域前端部署一台防火墙。通过核心业务域防火墙的入侵防御、僵尸网络识别等安全防御功能，就能阻断来自其他内网区域对核心业务域的非法攻击。

④对外服务域：该区域主要包括有提供对外服务的系统服务器，包括站群系统的前端服务器、Web 业务服务器等。通过在该区域前端部署一台 Web 应用防火墙，在网络层、WEB 服务层、应用程序层、应用内容四个层面提供全面的安全检测与防御，以应对通过外联区域针对 Web 服务的各种渗透攻击。

⑤终端接入域：顾名思义，内网中接入各种终端设备的区域，通过上网行为管理系统对接入校园网的用户终端进行认证上网访问控制，明确访问权限以及可访问的网络范围，并通过出口防火墙和态势感知系统及时发现失陷或者存在风险的终端。

⑥安全管理域：安全管理域是通过安全感知平台、日志审 计、运维审计、基线核查等系统对全网进行安全管理的区域。根据等保2.0 的相关技术要求，学校需要在安全管理域部署运维管理系统（堡垒机）、数据库审计系统、综合日记审计系统、物联网平台、综合探针和态势感知平台。

## 5.3 加入网络安全态势感知技术

网络安全态势感知技术可以帮助解决安全防护系统缺乏主动性、完整性、缺乏可视化等问题，是近年来非常流行的技术。

### 5.3.1 网络安全态势感知技术的现状

参考马航航的高校校园网网络安全态势感知建设方案一文，态势感知技术是一种基于环境的、动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全 局视角提升对安全威胁的发现识别、理解分析、响应 处置能力的一种方式，最终是为了决策与行动，是安全能力的落地。网络安全态势感知主要分为要素提取、态势理解、态势预测三个层面，利用数据融合、数据挖掘、智能分析和可视化等技术，直观显示网络环境的实时安全状况，为网络安全提供保障。网络安全态势 感知从提出至现在一直是网络安全领域的研究热 点，随着相关技术的不断完善，网络安全态势感知逐步走向成熟。

### 5.3.2 网络安全态势感知技术的架构设计

整体逻辑架构分为数据采集、大数据平台、检测分析、应用展示四层逻辑架构，各层级以及模块之间的功能设计具有相对的独立性，并且整个系统具有较高的扩展性，如图所示。

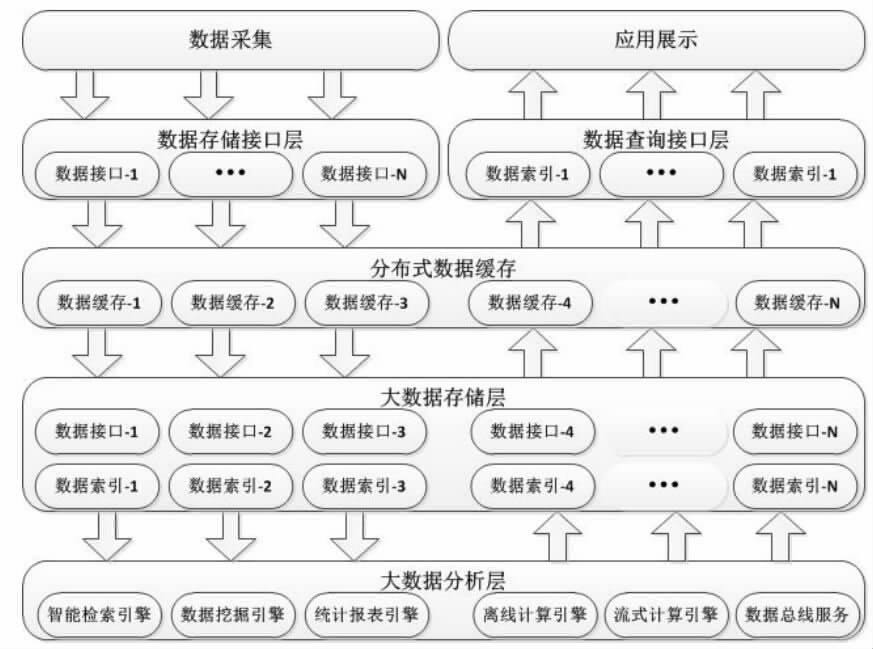


#### 5.3.2.1数据采集

数据采集主要通过采集器、流探针对数据源的日志/流量进行采集和预处理。 数据源包括安全设备、网络设备、日志服务器、应用主机等。通过优化的多管道并发处理机制，日志采集器把Syslog日志、Netflow数据和第三方日志按照统一的归一化数据格式进行转换，统一转存到大数据平台，支持安全事件分析、威胁呈现、追踪溯源等。部署的流探针和防火墙内置流探针负责原始流量采集，提取原始流量的协议特征，实现流量数据采集和协议还原。

#### 5.3.2.2大数据平台建设

大数据平台为整个态势感知系统提供数据存储和索引的功能，负责接收数据采集层传出的日志和流量数据。大数据层可以分为数据存储接口，数据查询接口层，分布式数据缓存层，大数据存储层和大数据分析层，如图所示：



①数据存储接口层针对不同的文件类型，像数据采集层提供接口，然后调用分布式数据缓存的接口将数据缓存。

②分布式数据缓存层可以缓解在数据查询高峰时带来的性能压力，减少数据查询的延迟。

③大数据存储层负责分析归一化之后的数据，并根据数据的特性建立索引，最终将其保存在物理存储介质中。

④数据查询接口层在数据缓存层和外部应用之间，向外提供数据查询接口，外部应用通过调用其接口得到所需数据。

⑤大数据分析蹭也就是检测分析层，在检测分析层部分展开描述

#### 5.3.2.3检测分析

使用深度学习，机器学习和强化学习等技术结合传统技术得到不同类型的分析引擎，例如流式计算引擎，统计分析引擎，规则引擎和关联分析引擎。这些引擎中内置很多分析规则，再结合大数据平台提供的日志和流量数据，通过不同的检测方式，如实现风险脆弱性安全预警溯源等分析，检测出潜在攻击和威胁。

#### 5.3.2.4 应用展示

应用展示层定制实现安全事件预警、安全设备联动、溯源、可视化等功能。安全事件预警主要针对海量日志数据和流量数据进行深层次的分析，发现数据中存在的关系和规则，发现潜在的安全威胁和攻击，预测校园网网络安全的发展趋势。安全设备联动从海量文件、流量和日志中识别检测出已知/未知威胁，生成联动策略下发给防火墙、IPS、WAF等网络安全设备，在网络侧进行阻断，并可将检测结果同步到终端安全设备，在终端进行检测并清除威胁。溯源通过关联分析、同源分析、机器学习等技术对大数据平台存储数据进行数据挖掘，支持基于攻击链进行事件调查，通过不同的攻击阶段关联流量元数据还原攻击原貌，并可通过网络行为的线索扩展发现攻击所用的网络资源、攻击者信息、受害人信息等线索。 可视化将碎片化的安全事件数据结构化，能以图表的形式实时在大屏上展现网络的攻击情况，准确定位出攻击源、攻击路径、攻击目标，快速找出安全威胁，直观显示校园网的网络安全状态。

#### 5.3.2.5部署方案

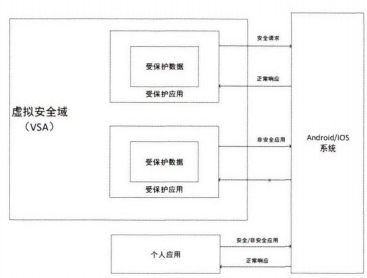
校园网网络安全态势感知建设方案组网部署如下：在安全管理域区部署CIS平台和沙箱，在互联网出口域部署流探针，在核心业务域、对外服务域和终端接入域部署服务器探针和终端探针。

## 5.4 基于虚拟安全域技术的移动办公解决方案

为了有效解决对移动端安全防护系统的忽视，需要打造一个安全防护性高、用户体验好，可扩展性强的移动安全平台。本文参考引用了哈尔滨工业大学（深圳）建设的一个基于虚拟安全域技术的移动办公平台：

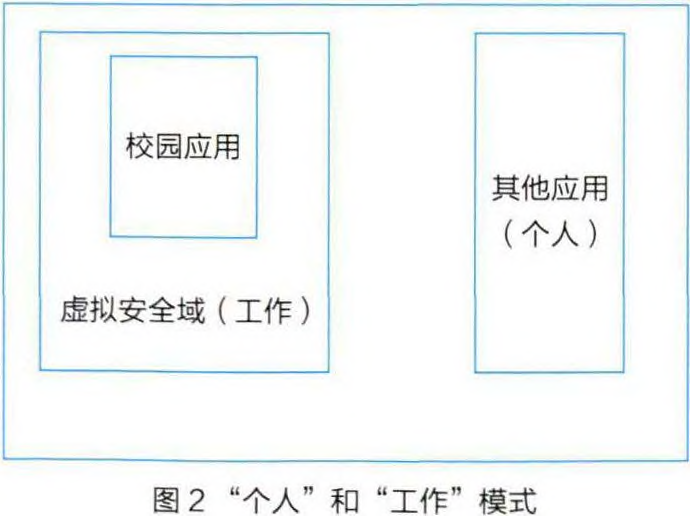
### 5.4.1虚拟安全域

参考哈尔滨工程大学虚拟安全域守护移动应用一文，“虚拟安全域（Virtual Security Area. VSA）,这是一种通过在系统底层实现提供移动应用安全保护能力的技术，无需获取应用源代码，也不需要Root权限；在代码零改造的基础上对应用形成的一个虚拟安全域。在该安全域中可实现各种移动业务安全运行的通用性需求：数据防泄露、应用功能安全调用、运行安全保护和隐私类保护等，也可以快速地适配实现其他个性化的网络安全保护和内容审计等需求用户将机密数据控制在一个安全的区域，能够了解用户的上网行为模式和进行行为监控，在学校开展移动业务的同时能够保证业务的安全运行。虚拟安全域技术的原理是通过VSA实现建立一个单独的、安全的虚拟系统，构建在应用和系统之间的桥梁。从系统底层对应权限和用户使用行为等进行全方位的管理和保护应用发起的请求先经过该安全虚拟系统中进行安全判断和审计，阻断不安全请求。防止将应用中的机密信息外泄等情况，使学校应用运行在一个安全可靠的环境中。”逻辑结构如图所示：



### 5.4.2构建内部移动应用商店

可以在虚拟安全域的概念上，建立一个学校内部应用商店，避免外部应用商店的复杂流程自行管理发布和审核APP，保护学校内部应用资产。内部应用商店相当于创建了一个虚拟安全域，通过将学校内部商店和外部商店的APP分开，就可以做到个人数据和企业政务数据的安全隔离，实现一个设备兼容工作和个人两套区域。这种统一管控的模式，让校园APP运行在虚拟安全域中，其他APP正常运行在系统上，就像有两个独立的逻辑空间，如图所示：



### 5.4.3防护模块

虚拟安全域并不能解决所有的问题，也还需要集成相关安全防护模块’包括的

模块有网络安全访问、上网内容审计、功能安全调用、隐私保护等，可根据不同业务场景配置不同的安全策略。