校园网的主动防护策略配置实例 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/293/2021_2022__E6_A0_A1_E5_9B_AD_E7_BD_91_E7_c67_293373.htm 学校校园网系统的具体情况是： ● 就以往的安全管理来看，以整体防御确保每一台计算机的安全对于学校来说只存在理论的可能性，实践起来较为困难； ● 学校只有一个专职网管人员而且脱离教学任务，对实际情况掌握的不是很熟悉。只能完成网管中心的局部安全； ● 就功能而言，学校的计算机网络可分为4大类型：教师集中办公的微机网络、学生上机的微机网络、网管中心网络、学校职能部门例如档案室、会计室、校长室、试卷库等部门网络； ● 学校了解网络安全的专业教师非常多，而且专业各有特长； ● 网络安全课程必须开设，内部攻击不能从制度上禁止。 分区防守，增强“ 壁垒 ”根据以上具体情况结合网络安全问题我们得出了以下的分析结果： 1、靠网管一个人实现整个网络的安全是不可能的。 2、四个不同功能的网络对网络安全的要求是不同的。教师网络因为权限较大所以主动染毒性非常强，但是由教师网络发起的对校园网络的内部攻击非常少。网管中心的网络非常重要但是相对安全。学生机房由于纪律的约束，主动染毒性不存在,但是针对网络的内部攻击次数非常多。学校职能部门网络由于涉及到学校的重要信息以及相关考试的信息，所以对网络安全要求非常高。 3、如果仍然采用习惯的整体防御，会出现一个区域网络安全出了问题导致其他功能区域全部出现问题。 针对学校的具体情况和网络安全问题的分析，我们制定了分区域防守与增强网段“ 壁垒 ”的总体安全策略。具体策略如下：

1、 由专业教师包括网管在内组成网络安全小组负责校园网络安全。小组成员根据专业方向的不同负责对威胁网络安全因素的具体防守，从人员方面加强力量。 2、 针对功能不同的网络，例如教师网络、学生网络等进行网络分段，分区域进行防守，不同区域根据安全问题的不同侧重采取相应的网段安全策略。 3、 整个网络安全体系由主防火墙和子防火墙一起构成。主防火墙由网管负责，进行网络整体防守。子防火墙由专业老师具体负责，配置到具体网段进行区域防守。 4、 不同的区域就是网段配置不同的五大安全部件，在防火墙、防毒墙、身份验证、传输加密、IDS/IPS几个方面区别配置来适应不同区域的具体要求。 以上就是分区域防守思想，我们在具体实施之后发现网络安全有以下几点可喜的变化： 1、校园整体网络安全有所提高，不同区域的网络安全由具体人负责，责任到人，相关网络安全问题可以快速解决。 2、因为专业人员的方向不同，负责不同区域的防守个人的专业特长有所体现，处理问题得心应手。 3、在出现安全问题时可以轻松做到尽量减少损失。在损失掉一个区域之后其他区域仍有很强的安全性，以往整个网络同时出现一种安全问题的现象基本杜绝。 4、成立了安全委员会后，负责不同防守任务的人员互通情况相互促进学校安全人员的技能和素质有很大的提高。 但是，简单的靠IP分段会存在许多功能问题。而且由于IP的人为可设置性使得网络存在很大的安全隐患。所以在此基础上学校更换了主交换机和子交换机。使用了主三层交换设备和可配置VLAN的子交换设备和高性能路由器。这样使得我们的分网段实施“ 壁垒 ”的思想可以更方便地实现。分网段实施“ 壁垒 ”的思想是分区域防守的有利保证

，从硬件方面增强了分区域防守的力度。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com