# 网络安全为校园　网络安全靠校园

## ——校园网络安全及防范措施

每年因黑客入侵、计算机病毒的破坏给企业造成的损失令人触目惊心。人们在享受到网络的优越性的同时，对网络安全问题变得越来越重视。

学校是以教学活动为中心的场所，网络的安全问题也有自己的特点。主要表现在：

**1. 不良信息的传播。**

在校园网接入 Internet 后，师生都可以通过校园网络在自己的机器上进入 Internet。目前 Internet 上各种信息良莠不齐，有关色情、暴力、邪教内容的网站泛滥。这些有毒的信息违反人类的道德标准和有关法律法规，对世界观和人生观正在形成的学生来说，危害非常大。如果安全措施不好，不仅会有部分学生进入这些网站，还会把这些信息在校园内传播。

**2. 病毒的危害。**

通过网络传播的病毒无论是在传播速度、破坏性和传播范围等方面都是单机病毒所不能比拟的。特别是在学校接入 Internet 后，为外面病毒进入学校大开方便之门，下载的程序和电子邮件都可能带有病毒。

**3. 非法访问。**

学校涉及到的机密不是很多，来自外部的非法访问的可能性要少一些，关键是内部的非法访问。一些学生可能会通过非正常的手段获得习题的答案，使正常的教学练习失去意义。更有甚者，有的学生可能在考前获得考试内容，严重地破坏了学校的管理秩序。

**4. 恶意破坏。**

黑客技术对校园网络系统进行破坏。表现在以下几个方面：对学校网站的主页面进行修改，破坏学校的形象；向服务器发送大量信息使整个网络陷于瘫痪；利用学校的 BBS 转发各种非法的信息等。

## 校园网安全的防范措施

目前，比较成熟的网络安全技术产品有：防火墙、入侵检测、身份认证、病毒防范、信息过滤、数据加密、VPN、VLAN、容错、数据备份、地址绑定等。但网络安全不只是这些技术产品的简单堆砌，它是包括从系统到应用、从设备到服务的比较完整的、体系性的安全系列产品的有机结合。

**1. 根据用户的特性和需求划分 VLAN**

校园局域网与其他企事业单位的局域网相比，联网计算机及网络用户的群体更为复杂。有教师备课机、学生机房、学生宿舍、图书馆、家属区以及人事、财务、后勤等行政办公计算机等。不同的用户对于网络有着不同的需求，对于自身信息的安全性要求也不同，据此可以将校园网划分为多个 VLAN。

**2. 在校园网出口设置防火墙网关**

防火墙网关能有效隔离校园网和外部互联网，使校园网与互联网之间的访问连接得到有效控制，阻止黑客对校园网的非法访问和攻击。针对校园网中部分重要的网段(如院长办公室、教务、财务、人事、科研中心、重要实验室等)设置防火墙网关，将他们和学生机房、学生宿舍及家属区的网段隔离，提供最基本的网络层的访问控制，使之不会受到来自校内其他网段的攻击。

**3. 合理运用入侵检测技术**

入侵检测技术是主动保护自己免受攻击的一种网络安全技术。作为防火墙的合理补充，入侵检测技术能够帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、攻击识别和响应），提高了信息安全基础结构的完整性。可以利用入侵检测技术构架校园网的主动防御体系，加强对校园网特别是行政、教研、服务器等重点网段的保护。

**4. 设置访问控制管理系统和智能信息过滤系统**

在学生上网比较集中的网段(如学生机房、学生宿舍、图书馆等)，设置 Internet 访问控制管理系统和智能信息过滤系统，从技术上对学生的上网行为进行管理和监控，防止学生有意无意访问含有黄、赌、毒、暴力、邪教等内容的网站。另外，还要加强对学生的信息道德教育、法制教育及上网行为的管理，使他们不再主动上网浏览、下载、传播这类信息。

**5. 加强服务器安全设置**

服务器是校园网的核心设备，也是黑客们的主要攻击对象，所以它们要有最高的安全性。网络操作系统是校园网服务器系统中最重要的组成部分，用户通过使用网络操作系统来使用校园网络资源，所以服务器安全的前提是网络操作系统的安全。

**6. 加强防范，防止病毒泛滥**

要建立一个有效合理的病毒预防和查杀机制。通过在网络中部署分布式、网络化的防病毒系统，不仅可以让单机有效地防止病毒侵害，还可以使管理员从中央位置对整个网络进行实时状态下的病毒防护。

**7. 在防火墙内口上捆绑 IP 和 MAC 地址。**

在汇聚交换机上捆绑 IP 和 MAC 地址，在接入交换机上捆绑端口和 MAC 地址。通过 MAC 地址、IP 地址、交换机端口的双重捆绑，解决校园网中 IP 地址盗用问题和 IP 冲突问题。

**8. 容错和备份**

对于重要的服务器，可以进行双机热备、磁盘镜像；对于重要的数据信息，采用数据备份技术，要定期进行备份、存储，做到防患于未然。一旦出现系统瘫痪、崩溃，可通过备份的数据信息快速地恢复系统。

**9. 加强内部安全管理，提高用户的安全意识**

为了确保网络和系统的正常运转，应该建立严格的局域网管理制度和机房上机管理制度，杜绝人为因素造成网络不安全。配备相应的网络管理人员负责整个网络安全的日常管理及维护。