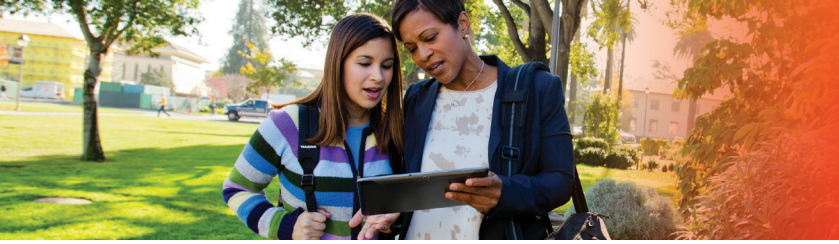


# 保护高等教育开放网络：
# 防御后 PC 时代的新威胁

## 概述

在高等教育领域，网络安全必须达到很好的平衡，因为高校非常重视开放式环境的价值。要对所有设备和流量类型开放，您不仅需要保护校园网络、信息和信誉，还需要响应各种请求，以识别参与非法文件共享活动的学生。

本白皮书专门面向高校的 IT、网络安全和合规性团队领导者，详细阐述应对下列高等教育安全挑战的可靠方法：

- 针对在校园中使用自带设备的学生进行恶意软件防护。
- 监控连接到学生宿舍楼网络的游戏机的使用情况，并限制其带宽消耗。
- 确保不会在无意中成为出站垃圾邮件中继点。
- 响应传票要求，确定违反《高等教育机会法案》(HEOA) 点对点文件共享规定的学生。
- 简化无线访客接入。
- 在适当情况下阻止个别学生接入。

## 在 BYOD 时代阻止恶意软件

**挑战**：假期结束后，学生们带着各种新设备（智能手机、平板电脑、笔记本电脑、游戏设备等）重返校园。 这些设备在连接到学生的家庭网络或公共网络时可能会受到感染，导致在随后连接到校园网络时传播恶意软件。在学生们自己拥有终端设备的情况下，传统的恶意软件防护方法（在终端设备上安装防病毒代理）并不可行。即便如此，从新病毒出现到防病毒供应商更新其特征文件这段时间里，恶意软件仍然可以偷偷潜入网络。

**解决方案**：解决方案是在网络层面而不是在设备上阻止恶意软件。思科® 安全架构提供多个选项来完成此任务：

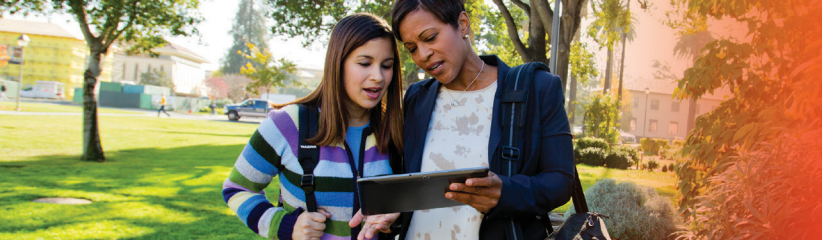
- 思科身份服务引擎 (ISE) – 识别用户身份和设备配置文件。
- Cisco ASA CX 情景感知安全 – 针对网络流量、Skype 流量、点对点流量及语音流量提供全面的防火墙功能和控制。
- 思科网络安全设备 (WSA) – 防御恶意软件并提供数据丢失防护。为获得全面且最新的威胁信息，该设备会连接至思科安全智能运营中心 (SIO)（参见侧栏）。
- Cisco ScanSafe 网络安全服务 – 在云中提供与 Cisco WSA 相同的保护，将设备和软件的资本支出转化为运营支出。
- 僵尸网络流量过滤器 – 这是 Cisco ASA 自适应安全设备的一项功能，用于帮助识别和阻止僵尸网络。僵尸程序会被暗中安装在受感染的校园网络，将命令和控制流量发送回攻击者的主机，从而窃取数据或发动拒绝服务攻击。僵尸网络流量过滤器监控网络端口以识别僵尸程序，并使用来自思科 ISO 的信息准确识别命令和控制主机。某大学目前使用此功能识别受影响的机器，为校园安全团队提供相关列表，并阻止命令和控制中心的“回拨”连接。通过此方法，该大学能够在不影响学生自由使用互联网的情况下改善其安全状态；只阻止流向已知的命令和控制中心的流量。

### 涵盖最新恶意网站的全面防御

**思科安全智能运营中心 (SIO)** 可防止高校遭受可能造成网络中断或使黑客能够检索机密信息的新兴威胁。凭借思科多达 1 亿美元的投资，SIO 可为高等教育机构提供以下优势：

- Cisco SensorBase 是一个威胁监控网络，它从全球部署的超过 70 万个思科传感器捕获威胁遥感勘测数据，监控全球 35% 的邮件和网络流量。 这些实时数据将与包含超过 4 万种漏洞的历史数据库相结合。
- 思科威胁防御运营中心配备 500 名安全分析师和自动化系统。这些分析师位于美国、澳大利亚、中国、印度、以色列、乌克兰和英国等国家/地区，全天 24 小时对新兴威胁进行研究。
- 动态更新可在几分钟内发送到您的思科安全设备（通常在其他解决方案几小时之前），使校园网络免受最新威胁的攻击。



## 管理学生宿舍楼威胁

**挑战**：游戏机很可能会接入到学生宿舍楼网络 (ResNet)。据说，在某大学因游戏机易受恶意软件攻击而试图禁止游戏机时，学生父母纷纷致电大学校长投诉，表示玩游戏对减轻压力很有帮助。跟踪游戏机给校园 IT 团队带来了挑战，因为它们不作为 802.1X Supplicant 向网络验证身份。校园 IT 团队还需要设法防止游戏机消耗过多带宽，导致宿舍其他房间的网络性能下降。

**解决方案**：使用 Cisco ISE 监测和控制游戏机使用情况。除打印机、传真机、笔记本电脑等设备外，Cisco ISE 还可以识别游戏机。当一台新的游戏机试图连接至 ResNet 时，Cisco ISE 会识别出该设备，并显示一个网页，要求学生注册该设备。您还可以限制每个学生的游戏机数量。

Cisco ISE 会显示每台设备是处于打开状态还是关闭状态。如果您看到一个 IP 地址正在生成过多的流量，您可以确定它是否是蓝光播放器、PlayStation 等设备，然后查看自助服务注册信息，了解谁拥有该设备。然后您可以要求该学生减少该游戏机的网络使用量，或将其从网络中断开。Cisco ISE 趋势报告有助于防止未来出现问题。例如，如果您从一份报告中看到连接到 ResNet 的 250 台游戏机消耗了 10% 的带宽，您可以将 Cisco ISE 与第三方工具配合使用，实施速率限制。

## 不要成为垃圾邮件发送者

**挑战**：在校生和已离校的学生拥有的受感染设备有可能成为垃圾邮件的出站中继点。如果发生这种情况，您的运营商可能会阻止来自大学 IP 地址的出站电子邮件，使运营中断并影响机构信誉。未受控制的大量电子邮件传送还会使收件人域（包括系统中的其他校园）不堪重负。

**解决方案**：思科邮件安全设备提供两种用于防止出站垃圾邮件和保持良好信誉分数的方法：

- 开启病毒爆发过滤器。
- 使用目标控制功能设置速率限制。您可以指定最大并发连接数、可发送至每个目标域的邮件数，以及收件人数量。

## 简化访客接入

**挑战**：校园 IT 团队通常需要在校友返校节（许多父母和校友来校园）等活动期间提供访客接入。常用的方法是在活动开始前创建数百个访客帐户，这些帐户需要逐一设置，十分耗时。

**解决方案**：Cisco ISE 可在访客尝试进行连接时自动注册访客，将流量限制在仅提供互联网接入的访客 VLAN。这样一来，校园 IT 团队可无需发放密码。

## 响应与非法的点对点文件共享相关的传票要求

**挑战**：《高等教育机会法案》(HEOA) 中包含一些旨在减少通过点对点文件共享方式非法交换版权著作的条款。但是，有些学生会违反此法律。因此，校园合规团队需要采用一种简单的方法来响应传票要求，以识别与非法文件共享活动 IP 地址有关的校园用户。但是由于 IP 地址经常变化，所以查明哪个学生在特定日期具有哪个 IP 地址非常困难。此外，一些机警的参与非法文件共享活动的学生可能会使用代理匿名器。

**解决方案**：一种方法是控制点对点应用（如 Tor 和 BitTorrent），并控制或阻止代理匿名器。您可以使用 Cisco ASA CX 情景感知安全解决方案来实现这种机制。或者，如果您的高校选择不阻止任何类型的流量，那么在原则上，您可以将流量与用户名相关联（而非与 IP 地址相关联），以便更轻松地响应传票要求。

## 限制特定学生接入互联网

**挑战**：高校有时需要采用别具一格的方法，让欠缴罚款的学生或反复违反点对点文件共享限制的学生加以注意。

**解决方案**：对现在的学生来说，引起他们关注的一种有效方法是中断其互联网接入。您可以通过将 Cisco ISE 集成到 Microsoft Active Directory 来达到此效果。例如，如果某个学生有多个未付款的违规停车罚款单，校园安全团队或 IT 团队可以选中该学生的 Active Directory 帐户所对应的复选框。当该学生下次尝试连接时，Cisco ISE 会发现该操作，并随即显示一个网页，说明在该学生支付罚款后才能恢复互联网接入。然后，Cisco ISE 甚至可以将连接重定向至学生可以支付罚款的页面。

## 总结

在后 PC 时代，高校面临一系列新的网络安全挑战。对每项挑战实施安全点解决方案并非可持续的方法，当新类型的威胁出现时，校园仍会处于易受攻击的状况。更具成本效益且更简单的方法是实施一种能够应对所有网络安全挑战的安全架构，例如恶意软件拦截、新设备（如游戏机）注册、防出站垃圾邮件和访客接入。

思科安全架构可满足所有这些安全需求，帮助高校在不影响校园信息和网络安全的情况下，保持其对开放式环境的承诺。

## 更多详情

要了解有关思科高等教育安全解决方案的详情，请访问 www.cisco.com/go/edumobilitywireless。

要了解有关思科教育解决方案的详情，请访问 www.cisco.com/go/education。