Hillstone 山石网科

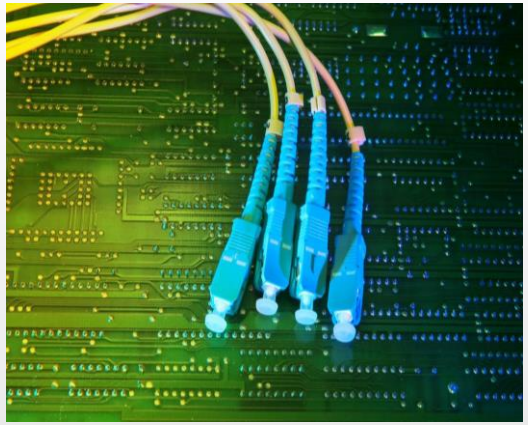
方案名称：某高校边界安全防护

个人信息：刘世鹏-陕西腾硕信息技术有限公司

背景介绍

某高校网络由于只搭建了最基础的网络架构，未作任何安全防护，导致校园学生资料以及校园网络安全性不高，校园介绍网页频繁遭受攻击和网络篡改，导致学校负面影响较大。

需求分析—学校面临挑战



运营成本快速增加

学校出口互联网众多，吞吐量持续增长，高并发及安全性需要提升。

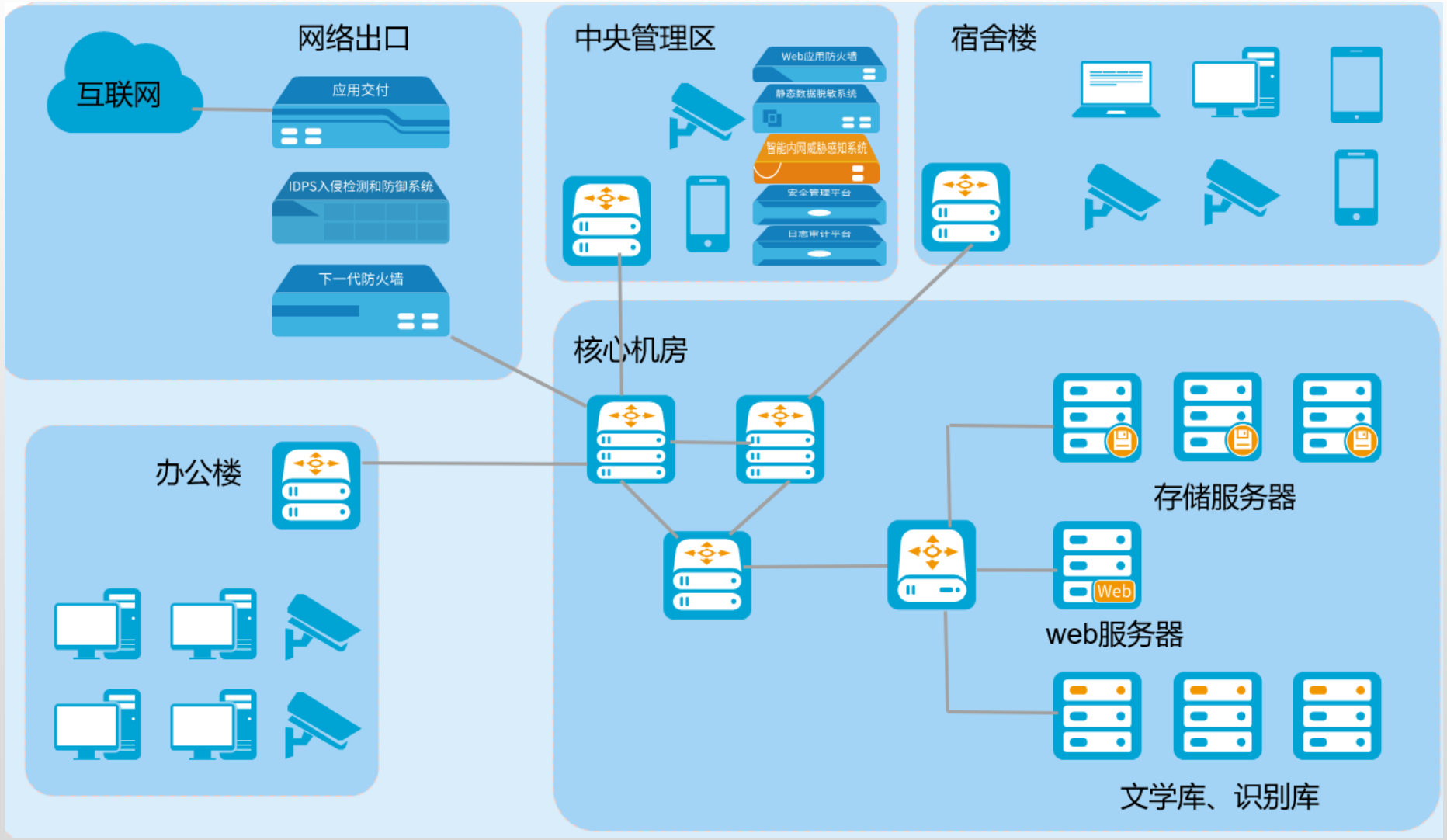
关键业务服务质量难以保障

学校互联网的设计重点需要从业务连续性保障， 延伸至通信服务质量保障， 满足各类应用系统客户使用体验高标准要求。

运维管理日渐复杂

传统的局部、碎片化的IT运维管理模式已经无法满足安全生产的实际需要。

解决方案—某学校核心机房安全防护方案



优势价值—山石网科安全防护

在中央管理区部署安全设备，例如web防火墙，静态数据脱敏系统，安全管理平台，日志审计及内网威胁感知设备。

1.web防火墙对学校网页介绍界面进行安全加固，防止非法篡改及故意抹黑的现象的产生

2.静态数据脱敏系统则对学校内部服务器的敏感数据进行防护，防止非法窃取等

3.安全管理平台则对多数产品的操作条件进行限制，确保不会出现其他人由于误操作而进入到设备管理界面进行非法操作

4.日志审计设备则对内网所有人员的网页访问记录及工作人员操作记录做统计，防止非法操作而无证据，并且也达到了国家要求保留日志达半年的条件

5.内网威胁感知则对内网终端设备进行风险扫描，检查并确认内网肉机，排除僵尸网络及其他相关威胁

6.网络出口处的IDPS设备则对系统漏洞进行打补丁，以及对内网与外网的数据流量进行病毒过滤和入侵防御的操作，确保不会有危险流量进入

7.防火墙则对高危漏洞直接封锁，并通过云沙箱功能对未知威胁进行验证扫描，并且可提供认证上网及流量检测，确保网络正常

8.应用负载则对流量进行负载均衡操作，确保业务流量正常转发，不会出现流量拥堵而造成业务慢等情况