

# Hillstone山石网科

## 普教城域网网络安全解决方案

### 一、普教行业现状描述

普教行业主要包含中学和小学，统一由区或县市的教委进行管理。随着多媒体计算机在教育过程中的应用越来越普遍，各地的中小学都普遍建设了自己的校园网络。普教老师可以利用校园网，对学生们开展丰富的多媒体网络教育，并利用Internet获得更多更及时的教育资源。

普教城域网将本地区各学校及教育机构通过网络连接起来，并与CERNET、INTRENET相连，在城域网上为本地区各学校提供可靠的、高速的和可管理的网络环境，为用户提供广泛的数据资源共享、丰富便捷的网络应用，实现网络的扩展，扩大联网的范围和规模，实现本地区“校校通”工程。

在分析普教城域网组网特点，结合各地普教城域网在建设、运维过程中遇到的一些实际问题后发现，存在以下安全风险和其脆弱性：

#### 1. 网络缺乏对多种攻击的有效防御

基于应用漏洞的攻击及不固定端口的应用挑战传统防火墙  
计算机病毒和网络病毒的肆意传播随时威胁着网络的稳定与安全  
ARP攻击泛滥导致整个网络访问瘫痪，缺乏有效控制和抵御措施

#### 2. P2P流量消耗网络带宽

P2P流量占网络总流量的六成以上，严重影响正常业务流量的带宽资源  
P2P软件逐渐成为计算机病毒和木马传播的主要途径  
需要对用户或者某些特定应用进行流量的控制

#### 3. 远程的安全接入

需要在远程办公、在家访问教育网资源时拥有安全快速的VPN接入

## Hillstone山石网科普教城域网网络安全解决方案

### 4. 对内网的监控以及内部用户上网行为进行有效控制。

需要通过监控流量、会话数、协议流量分析等途径分析网络运行状况和用户上网行为。

需要记录上网行为、论坛发帖等信息，做到严格控制和完全审计

### 5. 集中化统一管理功能缺乏

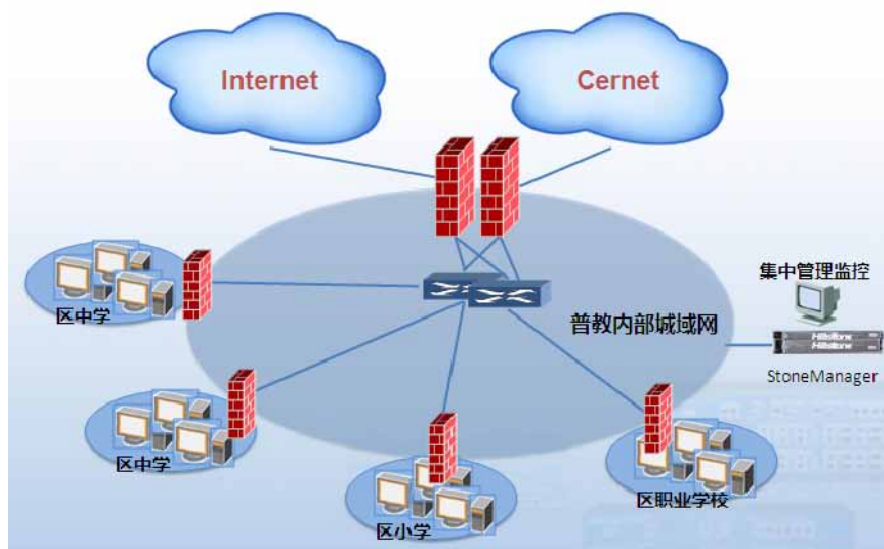
部署时需要统一的网络管理平台

希望通过统一管理平台看到网络中流量情况、会话情况、病毒感染情况及相关统计报表

## 二、Hillstone山石网科普教网络安全方案

综上所述，结合网络方案设计原则，通过分析普教网络建设中普遍存在的几点问题，我们提出如下解决方案：

某普教城域网安全解决方案示意图



### 1、通过Hillstone山石网科产品提供高性能的安全管控功能

网络攻击防护：Hillstone山石网科对于这类传统意义的攻击，凭借其多核并行处理的性能优势和应用层的攻击检测机制，能够将网络攻击识别防御。

ARP欺骗攻击防护：传统解决这种攻击的MAC-IP绑定的方式已经无法防御。通过

## Hillstone山石网科普教城域网网络安全解决方案

Hillstone山石网科的ARP防护解决方案，可以从几个方面解决这种攻击：

- Hillstone山石网科独有的SecureDefender安全客户端
- MAC-IP-PORT绑定
- 端口隔离功能
- 发送“免费ARP”广播和帮助其他主机发送
- ARP的反向查询
- 每MAC的IP地址数量限制

病毒防护：Hillstone山石网科与卡巴斯基合作，在安全网关产品上提供并行流引擎的高效率病毒检测，可对网络中威胁最大的病毒进行有效查杀并保障数据的快速传输。

IPS攻击防护：Hillstone 山石网科采用了全新一代基于应用行为和特征的应用识别，其基于深度应用识别的技术，突破传统基于端口的网络防御方式，真实的识别出流量对应的应用，从而有针对性的去防范针对应用的攻击。

### 2、通过Hillstone山石网科产品管理和限制P2P流量

对于教育行业普遍存在的互联网资源浪费问题，Hillstone山石网科提供专业QoS带宽管理解决方案来协助用户管理网络流量，杜绝单个IP占用流量过多问题，保障每个用户都有可用带宽。

Hillstone山石网科产品提供专有的智能应用识别(Intelligent Application Identification)功能，称为IAI。IAI能够对百余种网络应用进行分类，甚至包括对加密的P2P应用和即时消息流量进行分类。QoS首先根据流量的应用类型对流量进行识别和标记，然后根据应用识别和标记结果对流量带宽进行控制并且区分优先级。一个典型应用实例是：某学校有10M电信链路，经过设备的流量分析显示，P2P流量占线路带宽的80%以上，这对于校园网络来说很正常，但这种网络是不健康的，因为时效性很强的HTTP被挤压后网页打开速度会大大受限，邮件发送接收及普通的视频、文件传输也会受P2P流量过多而影响效率。通过在设备上的策略配置，可将网络中指定地址段的P2P总流量限制到10%之内，并对FTP、HTTP、SMTP、POP3等协议的带宽予以保障，由此可使网络效率提升，网页、邮件发送等延迟大大降低。

通过Hillstone山石网科提供的报表，可查看网络中占用带宽最多的IP地址或用户，占用带宽最多的应用类型，并能查看到某IP中应用协议的使用情况或某种应用协议中哪个IP占用最多的排名，方便网络管理者进行统计和分析。

## Hillstone山石网科普教城域网网络安全解决方案

### 3、Hillstone山石网科提供安全、可靠、便捷的SSL VPN远程访问

对于教师及员工系统在家办公及其他远程访问校内资源的需求，可以通过Hillstone的SSL VPN便捷的接入校园网。Hillstone的SSL VPN无需预先安装和配置客户端，所有的安装和升级都可以在远程接入时自动完成，这可以大大降低运维成本。同时集成了基于SSL的用户认证机制。配合USB-key认证、主机特征绑定、客户端安全检测等功能，可在提供数据传输安全的同时保障整网安全，减少网络中的安全隐患短板。

### 4、通过Hillstone山石网科产品提供灵活高效的上网行为管理

Hillstone山石网科安全网关对于校园网及庞大的教育城域网等用户群的认证、计费、审计、行为监控等需求提供统一管理。上网行为管理功能对网络游戏、在线聊天、在线炒股、P2P下载、网页访问、邮件外发及论坛发帖等各种网络行为进行全面控制管理，并可以根据需要针对不同用户、不同网络行为、不同时间进行灵活的管理策略设置和日志记录，同时能够配合集中网络安全管理系统（HSM）对网络行为日志进行查询统计与审计分析，从而为网络管理者的决策和管理提供重要的数据依据。

### 5、通过Hillstone山石网科实现整网设备的统一管理

HSM能够针对安全网关进行统一的集中控制和管理，包括日志收集、设备实时监控、历史数据汇总查询以及安全审计报表功能。其中对于设备的实时监控能够提供全面而灵活的网络信息，如通过HSM我们能够看到实时的设备CPU波形图、内存波形图、会话数波形图、VPN连接波形图、接口流量波形图、攻击波形图以及病毒防护状态波形图。

通过这些波形图或者柱状图我们能够清晰的了解到企业网络内部各个IP的流量情况、各个应用的流量情况，甚至能够看到一个特定IP内部各种应用的流量情况，对于用户网络管理员监控网络使用情况、定位网络问题以及优化网络结构都是必不可少的辅助工具。

#### 北京总部

海淀区上地七街1号  
汇众大厦3层  
邮编: 100085  
电话: 010-8289 7229  
传真: 010-8289 9814

#### 上海办事处

陕西北路1388号  
银座企业中心1715室  
邮编: 200060  
电话: 021-6149 8205  
传真: 021-6149 8001

#### 广州办事处

天河体育东路122号羊城国际  
商贸中心东塔15层1510-1511  
邮编: 510620  
电话: 020-3825 4309  
传真: 020-3825 4311

#### 成都办事处

总府路2号时代广场A  
座26层2625  
邮编: 610016  
电话: 028-6606 7115  
传真: 028-6606 7199

#### 南京办事处

中山东路300号  
长发中心A栋1602室  
邮编: 210002  
电话: 025-8682 9916  
传真: 025-8682 9916-606

#### 西安办事处

高新技术开发区科技路33号  
高新国际商务中心7层704B  
邮编: 710075  
电话: 029-8833 7347  
传真: 029-8833 7347