商业轻骑兵解决方案

教育行业教育城域网安全监管方案

开局指导

新华三技术有限公司

http://www.h3c.com

目录

官网介绍.....2

参考设备配置清单.....2

参考组网及关键技术.....3

开局相关资料.....4

官网介绍

https://www.h3c.com/business/jy4.htm

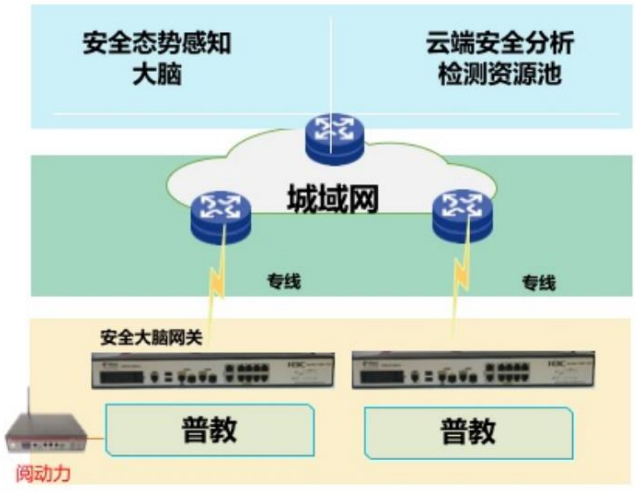
参考设备配置清单

教育城域网安全监管解决方案：

类型	组网应用定位	产品选型建议	备注
设备	城域网中小学出口防火墙	F1000-AK1010	
	探针服务器	网站扫描探针服务器	16核CPU,32G内存，1T硬盘。
		网络空间资产探测探针服务器	1万IP网络地址扫描：4核8线程CPU,32G内存，1T硬盘。
			10万IP网络地址扫描：8核16线程CPU,64G内存，2T硬盘。
			50万IP网络地址扫描：16核32线程CPU,128G内存，8T硬盘。
	专用硬件探针	流量探针	用来监测访问教育城域网的流量，软硬一体架构，ARM架构，系统具备足够的转发与数据处理能力，检测全面，对流量一次性完成入侵威胁检测、防病毒检测、应用识别检测、URL信誉检测、WEB攻击检测、威胁情报匹配检测。（按照局点流量吞吐选择合适款型）
	平台硬件	平台服务器	2颗CPU，单CPU主频≥2.1G，单CPU性能≥10核，内存≥256G，系统盘SAS HDD≥2*600G ,存储盘SATA HDD≥12*4T，千兆以上网卡:无具体型号要求，服务器能够识别即可（推荐NIC-GE-4P-360T-L3）；电源：2个800W交流电源

类型	组网应用定位	产品选型建议	备注
相关软件产品	安全态势感知	资产发现管理组件	对接网络空间资产探针探测的互联网资产数据，对接被监管单位上报的以及流量被动发现的资产数据，对属地网络资产进行全生命周期管理。
		安全监测感知组件	包括三大功能模块： 1. 实时威胁检测：以安全大数据为基础，从不同视角和维度进行风险呈现，实现安全事件实时监控与预警，发现潜在的安全问题，基于机器学习和专家系统，对大范围样本数据进行安全分析，发现威胁并预判趋势； 2. 网站安全监测：通过爬虫技术、沙箱技术、漏洞扫描等技术以云SaaS形态为客户提供主动的网站安全监控与检测，能够主动监控网站安全问题，监测网站脆弱性； 3. 网络异常行为：基于海量的数据，对资产进行分析，建模和学习，通过已经构建的规则模型、统计模型、机器学习模型和无监督的聚类分析，构建出资产在不同场景中的正常状态并形成基线，从而有效识别行为偏移，及时发现资产存在的可疑流量行为
		综合态势展示组件	提供整体威胁态势、外网攻击态势、资产态势、脆弱性态势以及通报态势等可视化呈现能力，帮助监管单位从宏观把控区域安全态势，加强统一指挥能力。
		业务安全运营组件	帮助上级监控部门了解各单位网络安全现状，为网信办进行统一指挥提供基础数据支撑，同时通过网信办和各单位的联动，实现以网络安全态势感知为基础推动网络安全工作的有效落地。
		重保指挥调度组件	在重要会议或重大活动期间，加强网络安保人员调度，全方位全天候掌握相关的单位、系统和网站安全状况，及时通报预警网络安全隐患，高效处置网络安全案事件。
		通报预警响应组件	协助监管单位对安全事件进行通报、反馈、处置，实现对业务安全的全闭环，支持被监管单位信息报送，帮助监管单位掌握信息安全状况，对通报事件进行全流程记录、跟踪，做到事后统计、复盘。
		应急响应处置组件	当发生安全事件的时候，可通过平台协同其他同级单位进行安全事件处置，通过建设事件处置基础资源库，通过平台向其他相关单位发送协同处置指令，利用基础资源开展攻击溯源、取证分析等工作，结合各方力量实现安全事件的协同处置，同时实现安全事件数据共享。
		融合联动共享组件	融合联动共享平台主要实现多源情报采集和自主上传、情报联动交换、情报共享推送等核心功能，包括多源情报聚合、多向情报分发、情报集成订阅等在内的多项应用能力。

参考组网及关键技术



方案名称	关键技术点	作用	涉及产品
教育城域网安全监管平台方案	下一代多业务特性	防火墙可以起多种安全防护效果：如链路负载均衡、SSL VPN、DLP、IPS、防病毒AV	F1000系列防火墙
	SCF虚拟化技术	可将多台设备虚拟化为一台逻辑设备，对外呈现为一个网络节点，资源统一管理，完成业务备份同时提高系统整体性能	F1000系列防火墙
	SOP 1:N完全虚拟化	可在设备上划分多个逻辑的虚拟防火墙，基于容器化的虚拟化技术使得虚拟系统与实际物理系统特性一致，并且可以基于虚拟系统进行吞吐、并发、新建、策略等性能分配	F1000系列防火墙
	全过程溯源取证	针对NAT应用场景，基于IP和时间段信息，追溯地址转换关系，并呈现对应的安全事件 利用云端丰富的实时威胁情报和本地的网络行为、终端行为、文件信息，覆盖攻击的源头、手段、目标、范围等相关信息，对发现的未知威胁进行快速溯源和定性	安全监管平台

开局相关资料

1. H3C SecPath F1000-AK 系列防火墙 快速安装指南-6W112

   https://www.h3c.com/cn/Service/Document_Software/Document_Center/IP_Security/FW_VPN/F1000-AK/Quick_Starts/Quick_Installation/H3C_F1000-AK_IQG/?CHID=363570

2. H3C SecPath F1000-AK 系列防火墙 其余资料：技术白皮书，用户手册，运行环境，技术介绍等参考以下链接

   https://www.h3c.com/cn/Service/Document_Software/Document_Center/IP_Security/FW_VPN/F1000-AK/?CHID=225398&v=612

3. H3C SecCenter CSAP 产品 快速安装指南-APW100

   https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Security/00Public/Quick_Starts/Quick_Installation/H3C_SecCenter_CSAP_IQG-APW100/?CHID=365637

4. H3C SecCenter CSAP 产品 其余资料参考

   https://www.h3c.com/cn/Service/Document_Software/Document_Center/IP_Security/SecCenter/H3C_SecCenter_CSAP/?CHID=288332&v=612