# 县级融媒体中心网络安全设备需求清单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **规格参数** | **单位** | **数量** | **全费用单价（元）** | **总价（元）** |
| 1 | 防火墙 | 1、防火墙吞吐量≥4Gbps，每秒新建连接数≥5万，并发连接数≥300万。 2、配置千兆以太网电接口≥16个，千兆光口≥8个，接口卡扩展槽个数≥2个，硬盘槽位≥1个。 3、要求单台配置硬盘≥500G，1U标准机架式设备，配置15个SSL VPN接入授权，实配内置固化双交流电源 4、支持一体化安全策略：可基于地址、端口、服务、应用、用户、时间、VRF等属性，配置入侵防御、数据过滤、文件过滤、防病毒、URL过滤、日志记录、会话老化时间等高级访问控制功能；（提供截图证明） 5、实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC和IP绑定功能，基于MAC的访问控制列表，802.1q VLAN 透传等功能。 6、支持DDoS 攻击防护，可防范多种类型DDoS 攻击，如SYN flood、UDP flood、ICMP flood、HTTP flood、DNS flood、ARP flood 和ARP 欺骗等。 7、支持DDoS流量阈值学习。启用学习功能后，系统将自动分析当前流量并计算出各种攻击类型的防范阈值，管理员可参考学习结果设置阈值。学习功能支持学习时长、学习模式、周期学习及自动应用等功能。（要求提供截图） 8、实现对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件、缓冲区溢出、SQL注入、IDS/IPS逃逸等攻击的防御，实现攻击特征库的分类。 9、基于特征检测，支持超过7800 漏洞特征的攻击检测和防御。（要求截图） 10、基于病毒特征进行检测，实现病毒库手动和自动升级，报文流处理模式，实现病毒日志和报表。 11、支持联动云端AV特征库进行全面实施核查（提供功能截图） 本地可检测病毒数量超过37000条。（要求截图） 12、支持Word、Excel、PPT、PDF、EXE、RAR等超过32种文件类型及内容的过滤。 13、支持海量预分类的URL地址库，支持根据URL类别实现URL过滤； 14、支持管理者自定义新的URL地址和URL分类； 15、支持联动云端URL地址库进行全面实施核查（提供功能截图）。 16、所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能，可独立分配CPU/内存等计算资源，虚拟防火墙可独立管理，独立保存配置（要求提供设备配置截图及官网证明截图）；虚拟防火墙具备独立会话管理、NAT、路由等功能。 17、在虚墙之内可配置VRF，支持二级虚拟化技术。（要求设备可测试，如中标后测试结果不满足，造成不利后果，保留法律追究责任） 18、实现N:1虚拟化技术，利用双机集群式高可靠性技术，融合后可统一管理配置，对外单一节点，实现主备/主主方式转发。（提供截图证明） 19、设备制造厂商符合能源管理体系ISO 50001:2011标准与电讯业质量管理体系TL9000认证，提供有效证书的复印件 20、设备制造厂商具备CNNVD（中国国家信息安全漏洞库）一级支撑单位资质，软件能力通过CMMI 5级认证，要求提供证书复印件 建议型号：H3C SecPath F1050 | 套 | 1 |  |  |
| 2 | 入侵防御 | 1、应用层吞吐≥2Gbps，新建链接≥3万，并发链接≥300万，固化提供不少于16个千兆电口，不少于8个千兆光口，设备扩展槽位≥2，自带双电源。 2、必须实配病毒查杀能力、流量控制能力、URL过滤能力、攻击防护能力 3、攻击特征库数量≥7500+、病毒特征库数量≥40000+、支持的协议识别数量≥3500+，提供设备界面截图证明 4、支持深入七层的分析检测技术，能检测防范的攻击类型包括：蠕虫/病毒、木马、后门、DoS/DDoS攻击、探测/扫描、间谍软件、网络钓鱼、利用漏洞的攻击、SQL注入攻击、缓冲区溢出攻击、协议异常、IDS/IPS逃逸攻击等 5、支持P2P、IM、视频等网络滥用协议的检测识别，支持的网络滥用协议至少包括迅雷、BT、eDonkey/eMule、Kugoo下载协议、多进程下载协议（网络快车、网络蚂蚁）等P2P应用， MSN、QQ、ICQ等IM应用， PPLive、PPStream、HTTP下载视频文件、沸点电视、QQLive等网络视频应用；可在识别的基础上对这些应用流量进行阻断或限流 6、支持专业防病毒功能，集成第三方专业防病毒厂商的专业病毒库，提供针对IPS产品的与专业防病毒厂商的合作证明 7、支持URL过滤功能，可以自定义需要过滤的URL规则，URL过滤可以基于时间、主机，能够精细到单一IP地址。 8、支持IP 碎片重组、TCP 流重组、会话状态跟踪、应用层协议解码等数据流处理方式 9、采用全面深入的分析检测技术，结合模式特征匹配、协议异常检测、流量异常检测、事件关联等多种技术，能识别运行在非标准端口上的协议，准确检测入侵行为 10、IPS检测到攻击报文或攻击流量后，支持阻断、限流、捕获原始报文等常规响应方式 11、IPS检测到攻击报文或攻击流量后，支持Web重定向、黑名单等响应方式，以实现第一时间隔离有安全威胁的主机，需提供配置界面截图 12、IPS可以针对不同的IP或IP网段应用不同的网络滥用带宽控制策略，针对不同网段应用不同的网络滥用带宽控制策略 可以识别并检测802.1Q、MPLS、QinQ、GRE等特殊封装的网络报文 13、支持特征库的手动、自动升级，特征库升级后设备无须重启即可生效（请提供设备管理截图） 14、系统具备对网站外链防护功能，可以对Web服务系统提供保护，需提供配置界面截图 15、系统应支持敏感信息防护功能，识别信息和文件中的关键字、身份证、手机号码、银行卡号、信用卡号等敏感信息，需提供配置界面截图 16、支持具备 DDOS自定义指纹防护，可根据报文长度、TTL值、源目的端口和 IP、序列号、flag标记等信息. 构成的正常流量模型进行指纹防护，并可根据用户需求设置相应的检测、防护阈值及多种防护动作，需提供配置界面截图 17、设备制造厂商具备CNNVD（中国国家信息安全漏洞库）一级支撑单位资质，软件能力通过CMMI 5级认证，要求提供证书复印件。 18、IPS产品在2018年IDC报告国内市场排名前三，提供有效证明文件复印件。 H3C SecPath T1030 | 套 | 1 |  |  |
| 3 | 上网行为管理 | 1、硬件要求：1U机架式独立硬件设备，≥4个Combo接口，≥10个GE接口； 2、内置2.4寸彩色液晶屏，具备触碰按钮；可显示版本号、CPU利用率、内存利用率、设备名称、管理IP等信息 3、网络吞吐量≥2Gbps；新建连接数≥8000 4、多核架构设计，非X86架构，功能采用模块化结构设计 5、制造厂商须为工信部ITSS全权成员单位，提供国家信息技术服务标准工作组ITSS全权成员单位证书复印件证明 6、IPSec VPN支持第三方对接和快速配置，自有设备对接时加密算法等参数无需配置，自动生成，仅需配置保护子网、共享密钥、IP地址，提供Web界面配置截图 7、支持自定义关键字对象，提供多种匹配模式，匹配类型包含关键字和数字，提供web界面配置截图 8、支持即时通讯应用管控的精细化管理，例如微信的“所有行为”、“语音”、“发消息”、“收消息”、“登录”、“发文件”等行为，并提供web配置界面截图 9、支持网络社区应用管控的精细化管理，例如可管控“所有行为”、“登录”、“网页浏览”、“发表”、“上传”等行为，并提供web配置界面截图 10、支持股票应用的行情和交易特征，并可以将股票软件的行情和交易进行区分管控，提供web界面配置截图 11、支持收集网站访问日志，记录用户所有访问网站行为；支持收集搜索引擎日志，记录用户的搜索内容；支持收集IM通讯软件日志，记录用户登录、收消息、发信息等行为；支持收集邮件日志，记录邮件发件人、收件人、主题、内容等信息，并提供web界面配置截图 12、支持单用户全天行为分析报表，一个界面同时展示用户名、用户组、在线时长、虚拟身份（如QQ号码、微博账号等）、日志关联情况、全天流量使用分布、网站访问类别分布、全天关键网络行为轴等信息，提供web界面截图 13、支持基于IP、端口、协议、URL对应用自定义 14、支持微信、QQ等即时聊天应用的聊天内容审计，提供web界面截图 15、支持HTTPS解密功能，支持管理界面及命令行配置解密策略，包括入接口、源地址对象、目的地址对象、https对象、域名排除等；支持HTTPS域名库，预定义域名以及自定义域名 16、支持审计HTTPS加密邮箱，支持审计主题、内容、附件等，支持本地下载邮件原件 17、支持针对HTTPS网站、HTTPS门户搜索等内容进行审计 18、支持通道化的QoS，支持基于源地址、用户、服务、应用、时间进行带宽控制，并支持配置保障带宽、限制带宽、带宽借用、每IP带宽、流量限额、带宽优先级等QoS动作，时间选择支持基于日计划、周计划、单次计划等。并提供web界面配置截图 19、所投产品须通过工业和信息化部审查，有《电信设备进网许可证》，具备CNNVD（中国国家信息安全漏洞库）一级支撑单位资质，软件能力通过CMMI 5级认证,能提供有效证书的复印件。 设备制造厂商符合能源管理体系ISO 50001:2011标准与电讯业质量管理体系TL9000认证，提供有效证书的复印件 建议型号：H3C SecPath ACG1000-SE | 套 | 1 |  |  |
| 4 | 硬盘 | 6T机械硬盘 用作服务器扩容 | 块 | 5 |  |  |
| 5 | ups | 中文液晶面板显示，显示输入输出参数电压、频率，并可直接在液晶面板上负载量、电池容量、输入输出参数及故障信息；输入电压范围（120vac～276Vac.旁路及ECO模式可设置；输入功因≥0.99，双市电输入；UPS输入频率范围（40HZ～70）±0.5HZ,能与任意发电机兼容，含底座 | 套 | 1 |  |  |
| 6 | ups输出箱 | 输入2\*C40A/3P 微断，输出6\*C40A/1P+1\*D20A/1P 微断，带电量仪，高 600\*宽400\*深240 | 台 | 1 |  |  |
| 7 | 电池组 | 16块12V/100Ah电池、电池柜、电池连接线1\*35、电池至UPS线缆、底座等。后备时间30分钟 | 套 | 1 |  |  |
| 8 | 系统集成 |  | 项 | 1 |  |  |
|  | 合计 |  |  |  |  |  |