**上饶市水利局网络安全等级防护设备**

**采购清单**

|  |  |  |
| --- | --- | --- |
| **设备名称** | **功能描述** | **数量** |
| 入侵防御 | 1. **功能描述**
2. 基本网络防火墙功能，IPSEC VPN功能，攻击防护，访问控制功能，用户认证功能，链路负载均衡功能、流量控制功能。
3. 关键字过滤和基于超过2000万域名的URL数据库可以帮助管理员轻松设置禁止访问的网页，控制对不良网站的访问，针对网络带宽、APP应用进行识别和管控。
4. 支持大病毒文件的扫描，实时病毒连接阻断，病毒事件记录，支持常见病毒传输协议HTTP、FTP及各种邮件协议扫描。
5. 基于状态、精准的高性能攻击检测和防御，实时攻击源阻断、IP 屏蔽、攻击事件记录，支持针对多种协议和应用的攻击检测和防御，支持SQL注入和XSS防御、外链防护和Web访问控制。
6. 支持独立的Web防护模块，提供防盗链、CSRF攻击、CC攻击、应用隐藏、网页防篡改等防护；支持HTTP协议的精确访问控制，可针对Method、Referer、User-Agent、Cookie、Url-args等字段设置内容。
7. 云端威胁情报订阅模块：提供攻击主机、僵尸网络、病毒木马、恶意软件、APT情报、恶意邮件等情报的活跃时间、可信度、家族分类，可应用于本产品的实时分析；设备支持针对内网进行威胁情报安全分析，跳转至威胁情报平台查询与溯源：云端提供对IoC威胁类型、多源情报、WHOIS、开放端口、SSL证书等多维度的溯源分析；云端服务：支持订阅高级威胁分析情报，云端提供最新APT入侵、0day漏洞预警、病毒变种情况等分析报告订阅。
8. **技术要求**
9. 标准1U硬件平台；双交流电源；含12\*GE电口,12\*SFP光口，500G硬盘，网络吞吐量8Gbps；最大并发连接数大于300万，每秒新建HTTP连接数大于10万。
10. 具备中国国家版权局颁布的《计算机软件著作权证书》
11. 具备全球IPv6测试中心颁布的《IPv6 Ready Phase 2证书》
12. 具备中华人民共和国工业和信息化部颁发的《电信设备进网许可证》
13. 支持实时获取威胁情报，并应用威胁情报对本地资产进行威胁检测，并可对检测到的威胁情报支持单点登陆威胁情报云平台查看该情报详情
14. 支持对最多20级的压缩文件进行解压查杀
15. 接口支持配置从属IP地址，每个接口要求支持至少200个从属IP
16. 支持4G接入，并可实现4G连接与有线链路之间互为备份；支持的4G网卡必须包括华为E3372；支持在4G接口上运行IPSec VPN
17. 支持DNS透明代理功能，代理算法包括：优先级、权重和流量
18. 支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL过滤、应用过滤、会话老化时间、终端过滤等高级访问控制功能
19. 支持应用识别，内置5000种以上应用特征库，并可识别iOS、安卓等移动互联网软件如微博、微信等特征，并可智能识别P2P和迅雷行为，并支持在线升级和手动升级
20. 支持智能和快速两种应用识别模式，在智能识别模式下应用引擎尽可能地用各种方式识别网络流量，在快速识别模式下应用引擎将关闭部分智能分析功能以提高性能
21. 提供邮件控制，支持针对邮件收发件人、邮件标题及内容关键字，邮件大小、邮件附件个数进行过滤；支持针对搜索引擎、HTTP上传、网页内容的WEB关键字过滤；
22. 支持针对虚拟账号过滤，设定允许登录的QQ账号白名单或禁止登录的QQ账号黑名单
23. 支持IP准入、MAC准入、IP+MAC准入、本地WEB认证、Portal认证、短信认证、免认证、微信认证、混合认证、AD域单点登录和访客二维码认证
24. 支持微信认证，可以选择获取IP地址、OpenID或手机号等实名信息，支持与微信公众平台进行认证联动，认证方式包括公众号按钮跳转、公众号回复关键词等方式。认证过程中要求用户必须关注公众号，帮忙单位实现品牌营销

需提供制造商参数确认函。 | 1套 |
| 日志审计 | 1. **功能描述**
2. 支持对工控网络设备、安全设备、操作员、业务应用系统等日志进行统一的收集及审计。
3. 支持对日志记录的统一收集、存储、分析、查询、审计和报表输出。
4. 支持对安全事件收集与积累并且加以分析，有选择性地对用户进行审计跟踪，及时发现可能产生的破坏性行为。
5. **技术要求**
6. 标准1U硬件，1个console口，资产授权数量：40个；网口类别：6个千兆口；硬盘：2T\*1；内存：8G；单电源日志处理能力2000EPS（峰值：4000EPS）；可扩展项：单个磁盘可扩展至4T(仅有1个盘位)。
7. 采用解决方案包上传对产品进行功能扩展，无需要代码开发；
8. 支持kafka日志接收转发、大数据安全域同步、APT沙箱报告转发等大数据联调功能；
9. 支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配；支持系统配置备份自动备份至远程服务器；
10. 支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等；
11. 三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件；
12. 通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息；
13. 支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警；远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并外发告警；
14. 用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户；
15. 支持分布式部署，支持页面一键添加子节点，自动进行绑定添加，采集器可以选择同步日志范围，按需转发数据。

需提供制造商参数确认函。 | 1套 |
| 杀毒软件 | 1. **功能描述**
2. 实现对终端的统一管理和策略下发，该管理中心需独占计算资源，不能与其他业务共享；
3. 对主机进行病毒查杀、漏洞管理、性能监控功能，在系统防护方面还可做到主动防御、系统登录防护、系统进程防护、文件监控，还支持网络防护、勒索挖矿防御、外设管理等。
4. **技术要求**
5. 支持对CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对CPU、内存达到一定阈值时客户端进行熔断。
6. 支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露；
7. 识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为。
8. 违规外联支持黑、白名单双模式，白名单模式可配置是否允许访问特定的网站和地址；黑名单模式可自定义恶意IP，支持黑名单告警和阻断。
9. 支持登录防护，包括以系统账号为粒度的异常登录防护、支持五个任意维度(任意地理位置，任意IP，任意域名，任意计算机名，任意时间)的系统登录访问策略设置。
10. 支持多引擎设置，包括默认引擎、深度扫描引擎；
11. 管理平台支持一键卸载客户端、一键设置客户端卸载密码、一键停止/恢复所有防护、一键解除绑定。
12. 支持对屏幕拍照泄密数据的行为进行溯源。
13. 产品适用于Windows PC防护支持Windows XP、Windows 7、Windows 8、Windows 10等操作系统并且支持不少于30台安全防护。
14. 机架式服务器，六核处理器，16GB DDR4内存，1块1T SATA 7.2K 3.5寸硬盘，支持RAID 0/1/5/6/10/50； 配置冗余电源，2个或以上千兆以太网口，支持虚拟化加速、网络加速、负载均衡、冗余等高级功能。

需提供制造商参数确认函。 | 1套 |
| 网络安全巡检服务 | 提供3年不定期对水利综合信息管理系统网络安全巡检、软件升级服务以及网络安全故障现场支持。 | 1项 |