**附件：江南水务网络安全建设项目询价采购需求**

**一、项目建设内容**

依据国家相关政策要求，对江南水务的信息系统进行安全建设，覆盖信息安全的管理体系、技术体系和运维体系三个方面，建设内容覆盖十个安全层面，即：安全物理环境、安全通信网络、安全区域边界、安全技术环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理。**二、项目建设清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **性能指标** | **数量** | **单位** |
| 1 | 安全感知平台 | 性能参数：存储容量：21.8T，在带宽性能1Gbps时存储时长：1200天/1Gbps。  硬件参数：规格：2U，内存：3\*32GB DDR4 2666，系统盘：1\*128GB SATA SSD，数据盘：8\*4TB，标配盘位数：8，电源：白金，冗余电源，接口：4千兆电口。  产品概述：  安全感知平台定位为客户的安全大脑，是一个集检测、可视、响应处置于一体的大数据安全分析平台，让安全可感知、易运营。 | 1 | 台 |
| 2 | 潜伏威胁探针系统 | 性能参数：吞吐性能：≤1.5Gbps。  硬件参数：规格：1U，内存大小：8G，硬盘容量：1T SATA，电源：单电源，接口：6千兆电口+2千兆光口SFP。 | 1 | 台 |
| 3 | 上网行为管理 | 性能参数：网络层吞吐量（大包）：3Gb，应用层吞吐量：300Mb，带宽性能：200Mb，IPSEC VPN加密性能（最高性能）：30Mb，支持用户数：1000，包转发率：27Kpps，每秒新建连接数：2400，最大并发连接数：120000。  硬件参数：规格：1U，内存大小：4G，硬盘容量：128G minisata SSD，电源：单电源，接口：6千兆电口+2千兆光口SFP。 | 1 | 套 |
| 4 | 工业安全管理与态势分析系统 | 工业安全管理与态势分析系统是一款基于大数据、机器学习等技术的企业级智能安全分析平台，通过收集工业网络内部各个关键设备或系统产生的业务数据，进行集中存储、快速检索、实时分析及告警、威胁响应、可视化展现和安全报告等功能。系统利用安全大数据的深度挖掘和机器学习智能分析等技术，为企业安全事件及异常行为检测、安全态势感知、运维管理和应用分析提供了一个智能、高效、可灵活扩展的解决方案。帮助企业发现和应对新型安全威胁，实现企业信息安全防御能力。提供资产脆弱性分析、日志集中分析、威胁模型构建、防护策略建议、风险预测、管理决策支撑等功能。2U机架式。含4个千兆电口，一个Console口(RJ45)。可扩展≥4个插槽。2个USB接口。内存64G，硬盘4\*2T，raid5。 交流单电源（可扩展冗余电源），风扇散热。10000条每秒单机。可选板卡:4千兆电口，2千兆光（单模,多模）。 | 1 | 台 |
| 5 | 工控主机终端防护 | 专用于保护工控主机环境的终端防护类产品，部署于工控上位机和服务器上，能防范各类已知和未知恶意程序的运行、控制USB移动存储介质的滥用、对主机系统进行安全加固等，实现对工控主机全面的安全防护。  （1）主机软件白名单防护、日志记录审计、支持微软32位/64位 Windows XP / 7/8/10等；（2）含安装授权 出厂包含三年软件版本升级服务，应急响应服务、远程支持服务； | 20 | 套 |
| 6 | 工业防火墙(机架式) | 面向工业控制网络，进行区域边界安全防护的硬件产品。产品基于对主流工业协议的深度解析，综合运用工控威胁特征识别技术、机器自学习与可信白名单技术，在提供传统防火墙的网络层控制和状态监控能力的同时，也可有效抵御各类针对工控系统的网络攻击和恶意破坏，为生产控制系统的稳定运行提供安全保障；1U机架式。含8个业务千兆电口，一个带外管理口，一个Console口(RJ45)。标配4组Bypass电口。2个USB接口。64G SSD（可扩展1T硬盘）。AC 220V 交流单电源（可选配增加为冗余电源），风扇散热。支持看门狗。网络吞吐量4Gbps，并发连接数300万，新建连接数8万。DPI吞吐量2G。 | 1 | 台 |
| 7 | 安全隔离与信息交换系统 | 基于“2+1”的硬件架构，确保高强度安全防护的前提下实现数据两网“摆渡”的功能，支撑http、ftp、工业协议、数据库等多种协议。2U机架式。含内网接口2千兆电口，外网接口2千兆电口，一个Console口(rs232)。单电源。最大吞吐量400M，最大并发连接数5万。 | 1 | 台 |
| 8 | 工控安全审计 | 面向工业控制网络，实时监测网络攻击和异常行为的硬件产品。产品采用工业级的硬件设计，利用黑名单、白名单、自定义规则等多种安全策略，通过内置的工控协议深度解析引擎，实时监测工控网络中违规行为、异常流量和不明设备接入，让用户实时全面掌握工控网络安全运行状况；通过完整的记录并留存工控网络流量，为事后取证和溯源分析提供依据。1U机架式。含4个业务千兆电口，4个业务千兆光口，一个带外管理口，一个Console口(RJ45)。2个USB接口。64G SSD+1T硬盘。AC 220V 交流单电源（可选配增加为冗余电源），风扇散热。支持看门狗。吞吐量500Mbps，并发连接数100万。含2个扩展插槽，可选板卡:4千兆电口，8千兆电，4千兆光，8千兆光，2万兆光，4万兆光。 | 1 | 台 |
| 9 | 安全增值服务 | 1：防火墙云端规则库更新服务，只能策略生成  2：IT网设备安全设备统一管理平台  3：安全运营服务：防火墙安全策略调优  4：微信专属管家服务：提供专属原厂服务人员进行服务，包括但不局限于设备运维问题，安全策略问题  5：安全意识培训服务，每年4次  6：安全应急演练服务，每年2次  7：安全风险评估服务，每年4次  8：安全漏洞扫描、分析及处置服务，每年2次 | 3 | 年 |

**三、技术参数**

**1、安全感知平台参数**

|  |  |
| --- | --- |
| **指标项** | **指标要求说明** |
| 硬件及性能 | ★存储容量≥21.8T，在带宽性能1Gbps时存储时长≥1200天/1Gbps。  规格：2U，内存≥96GB，系统盘≥128GB SATA SSD，数据盘≥8\*4TB，电源：白金、冗余电源，接口：千兆电口≥4个。 |
| 大屏可视 | 支持大屏展示综合安全态势，包括资产态势、脆弱性态势、网络攻击态势、安全事件态势、外连态势、横向威胁态势、设备运行态势，支持页面跳转到对应态势大屏，并具备大屏告警能力； |
| ★为清楚了解我司网络安全、资产以及遭受的攻击状况，在受到攻击时能及时告警，减少管理难度，要求设备支持支持综合态势、安全事件态势、通报预警态势、外部攻击态势、脆弱性态势、资产态势、设备运行态势等多个专项独立大屏展示功能，支持轮播，可根据我司环境自定义轮播顺序【提供功能截图，报价时以PDF格式上传】 |
| 资产中心 | 支持感知业务/服务器资产，可定义IP地址、所属分支、主机名、责任人、责任人邮箱、所属业务、操作系统、服务与端口等信息，并支持基于流量支持识别操作系统、开放的服务与端口。 |
| 支持感知终端资产，可定义终端/ip组、主机名、用户名、用户邮箱等信息，并支持基于流量自动识别终端。 |
|
| 脆弱性感知 | 支持基于流量检测业务服务器的风险端口开放情况，检测列表包含服务器、所属分支、协议与端口、总流量、流入流量、外网源IP TOP3、更新时间等，并支持导出风险端口报告 |
| ★为了减少因管理员策略配置不当而导致遭受黑客攻击，要求设备能够支持基于流量检测业务服务器配置不当情况，检测对象包含服务器、所属业务、配置不当类型、风险等级、发现时间等，支持展示配置不当详情，提供解决方案和数据包举证，并支持导出配置不当报告，以便我司管理人员及时修改【提供功能截图，报价时以PDF格式上传】 |
| 支持镜像流量检测web流量中是否存在可截获的口令信息，检测列表包含对应域名/URL、服务器IP，所属分支和业务，数据包举证等信息，避免因明文传输导致信息泄露的风险。 |
| ★由于主动扫描需定期进行、同时主动扫描因占用流量过高可能导致我司业务数据传输而影响员工正常办公，要求设备能够支持基于流量实时漏洞功能，其分析类型需包含配置错误漏洞、OpenSSH漏洞、目录遍历漏洞、OpenLDAP等操作系统、数据库、Web应用等，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告【提供功能截图，报价时以PDF格式上传】 |
| 处置中心 | 具备失陷(业务和用户)主机详细分析，包含攻击阶段分布、风险等级趋势、安全事件举证、遭受的外部攻击、存在的漏洞风险、行为画像（EBA）、开放端口等信息。 |
| 支持终端维度展示终端IP、所属分支、所属终端组、风险等级、安全事件标签、处理状态、联动状态，风险等级包含已失陷、高危、中危、低危、信息等。 |
| 分析中心 | ★为避免员工无意中使用携带了病毒的U盘或其他外设而导致的内部威胁扩散，要求设备支持横向威胁感知并展示横向威胁总览、横向攻击、违规访问、可疑行为、风险；其中横向风险总览包含发起与遭受横向威胁主机TOP5，发起视角包含但不限于发起者IP、发起者类型、所属分析、所属业务/终端组、横向威胁类型。 |
| 具备安全日志分析引擎、DnsFlow行为分析引擎、HttpFLow分析引擎、NetFLow分析引擎、MailFLow分析引擎、SmbFLow分析引擎、威胁情报分析关联引擎、第三方安全检测引擎、文件威胁检测引擎等，支持定期自动升级或离线手动升级 |
| ★为保障我司资产安全，避免遭受挖矿风险，要求设备具备挖矿专项检测，可实时查看挖矿各个攻击阶段，包括感染挖矿病毒、与控制端建立通信、获取挖矿任务、尝试挖矿、挖矿成功等；并支持挖矿币种分布、挖矿风险态势、受影响主机等维度分析统计，以便管理员及时进行维护处理【提供功能截图，报价时以PDF格式上传】 |
| 报告中心 | 支持展示需要处理的风险主机与风险状况报告，报告内容包括业务与终端风险摘要、业务风险与终端详情分析，提供危害解释和参考解决方案；适用于日常处理安全问题的运维人员。 |
| 支持分析具体的业务系统存在的脆弱性风险报告，报告内容包含脆弱性检测总览、业务脆弱性详情分析等，提供危害解释和参考解决方案。 |
| 支持完整展示网络的安全态势和详情的综合风险报告，报告内容包括平台说明、安全风险概括、业务与终端安全详情分析、安全规划建设建议等。 |
| 平台管理 | 因我司管理人员有限，为简化管理员运维难度，提高管理效率，要求：  ★1、平台能与本项目中行为管理对接，同步上网行为管理设备认证用户，避免多次认证的繁琐步骤，同时能实现与安全事件关联【提供功能截图，报价时以PDF格式上传】 |
| ★2、平台能够与我单位现有防火墙做功能对接，实现平台下发安全策略到防火墙，阻断攻击流量【提供功能截图，报价时以PDF格式上传】 |
| ★3、分析平台可对安全探针进行统一的升级管理，支持配置向导功能，通过系统检测功能，检测设备基础配置、设备资源、设备接入情况、设备流量等是否有异常，并导出上架检测报告，同时支持监控探针和各类安全组件的运行状态，其中安全组件需包括上网行为管理、防火墙【提供功能截图，报价时以PDF格式上传】 |
| 资质要求 | 具备公安颁发的销售许可证  厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位  ★厂商具备云安全成熟度成熟度模型CSA-CMMI 5认证  ★厂商具备软件开发成熟度CMMI 5级认证 |

**2、潜伏威胁探针系统参数**

|  |  |
| --- | --- |
| **指标项** | **指标要求说明** |
| 品牌要求 | ★与安全态势感知系统为同一品牌 |
| 硬件及性能 | 吞吐性能≥1.5Gbps，内存≥8G，硬盘容量≥1T SATA，接口：千兆电口≥6个、千兆光口≥2个。 |
| 资产发现 | 具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等 |
| 基础检测功能 | 具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等,  具备多种的入侵攻击模式或恶意URL监测模式,可完成模式匹配并生成事件,可提取URL记录和 域名记录,在特征事件触发时可以基于五元组和二元组(IP对)进行原始报文的录制。 |
| 监测识别规则库 | 能够识别应用类型超过1100种，应用识别规则总数超过3000条，具备亿万级别URL识别能力。漏洞利用规则特征库数量在4000条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应CVE编号； |
| 深度监测能力 | 可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP地址扫描，端口扫描，ARP欺骗，IP协议异常报文检测和TCP协议异常报文等常见网络异常流量事件类型; |
| 高级检索 | 支持DNS审计日志，主要用于平台dns flow分析引擎进行安全分析；HTTP审计日志，主要用于平台http flow分析引擎进行安全分析；SMB审计日志，主要用于平台SMB flow分析引擎进行安全分析；同步SMTP、POP3、IMAP审计日志，主要用于平台Mail flow分析引擎进行安全分析，同步AD域协议审计日志，主要用于平台AD域分析引擎进行安全分析； |
| Web应用安全检测能力 | 支持针对B/S架构应用抵御SQL注入、XSS、系统命令等注入型攻击；支持跨站请求伪造CSRF攻击检测；支持其他类型的Web攻击，如文件包含，目录遍历攻击等的检测；  支持敏感数据泄密功能检测能力，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤； |
| 管理功能 | 能够提供网络管理功能，可进行静态路由配置；  可支持在线升级和离线升级，并依托安全感知平台进行统一管控；  可实时监控设备的CPU、内存、存储空间使用情况。 |
| 集中管控 | 支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级； |
| 资质要求 | 具备公安颁发的销售许可证  厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位  ★厂商具备云安全成熟度成熟度模型CSA-CMMI 5认证  ★厂商具备软件开发成熟度CMMI 5级认证 |

**3、上网行为管理系统参数**

|  |  |
| --- | --- |
| **指标** | **具体指标要求** |
| 基础要求 | 网络层吞吐量≥3Gb，应用层吞吐量≥300Mb，带宽性能≥200Mb，支持用户数≥1000，每秒新建连接数≥2400，最大并发连接数≥120000。  内存≥4G，硬盘容量≥128G minisata SSD，接口：千兆电口≥6个，千兆光口≥2个。 |
| 部署 | 支持网关模式，支持NAT、路由转发、DHCP、GRE、OSPF等功能；支持网桥模式，支持旁路部署，多路桥接 |
| 支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置；  所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6 |
| 接入认证 | 支持绑定IP认证、绑定MAC认证，及IP/MAC绑定认证等；支持通过SNMP服务器跨三层获取MAC地址；支持绑定IP/MAC后，实现免认证 |
| ★支持二维码认证，担保人扫描访客的二维码后对其网络访问授权【提供产品截图或证明材料，报价时以PDF格式上传】 |
| 实时监控 | ★为了解我司员工上网状况，减少员工因网络质量差而导致的工作效率下降，要求设备能够针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级；支持以列表形式展示访问质量差的用户名单；支持对单用户进行定向web访问质量检测。【提供产品截图或证明材料，报价时以PDF格式上传】 |
| 支持PPS异常、丢包异常、ARP异常、内网DOS攻击等异常情况实时监测，显示每日异常事件个数及情况； |
| 应用管理 | ★为我司能够针对不同部门/员工进行精细化的应用管控，要求设备内置应用识别规则库，支持超过6000条应用规则数，支持超过2800种以上的应用，1000种以上移动应用，并能及时更新、保证应用识别的准确率及减少规则库占用的资源； |
| 为避免员工浏览微博、论坛、网盘以及聊天时有意无意的外发我司内部信息，要求：  1、能够对新浪微博、腾讯微博、网易微博等进行细分控制，如：登录、浏览、发微博、上传附件等；  ★2、能够对teamview、QQ远程桌面等远程控制应用做细分控制，如：接受对方远程控制【提供产品截图或证明材料，报价时以PDF格式上传】  ★3、能够对Github、百度网盘、百度文库等网络应用的上传动作进行细分控制【提供产品截图或证明材料，报价时以PDF格式上传】 |
| 支持记录QQ、微信传文件动作和传文件内容，并可记录传文件类型和文件长度 |
| 邮件管理 | 支持对加密HTTPS、POP3-SSL 、POP3、IMAP 、IMAP-SSL、SMTP-SSL、SMTP邮件内容的审计。 |
| 流量控制 | ★为避免员工在上班时间访问视频网站、下载视频等行为，要求支持通过抑制P2P的上行流量，来减缓P2P的下行流量，避免影响正常业务数据流量的传输【提供产品截图或证明材料，报价时以PDF格式上传】 |
| ★为了更好地对员工上网流量进行管控，让更多的流量用于公司重要业务的传输，要求基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中【提供产品截图或证明材料，报价时以PDF格式上传】 |
| 上网行为审计 | 审计SSL网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。解决管理员给每台PC单独安装证书的问题 |
| 记录QQ、微信传文件动作和所传文件内容，并可指定记录传文件类型和文件长度；支持同时审计QQ聊天内容和QQ传文件内容。 |
| 上网日志管理 | 设备必须支持内置数据中心和独立数据中心 |
| ★支持预置几组关键字，当审计日志中出现这些关键字时，将定期以邮件的方式发送报告给指定邮箱 |
| 支持与同品牌安全感知平台联动 | ★为简化我司管理人员运维难度，提高管理效率，要求能与本项目中安全感知平台对接，实现用户同步，以基于用户身份进行威胁分析【提供产品截图或证明材料，报价时以PDF格式上传】 |
| 资质要求 | 产品应具公安部颁发的销售许可证；提供有效证书的复印件。  国家标准《信息安全技术信息系统安全审计产品 技术要求和测试评价方法》的主要起草单位，提供有效证明材料复印件，报价时以PDF格式上传  公司研发体系通过国际认证CMMI5，提供有效证书的复印件。  国家应急中心应急支撑单位CNCERT证书（国家级）提供有效证书的复印件。 |

**4、工业安全管理与态势分析系统参数**

|  |  |  |
| --- | --- | --- |
| **指标项** | | **具体指标要求** |
| 基础要求 | 硬件要求 | 2U机架式。含4个千兆电口，一个Console口(RJ45)。可扩展≥4个插槽。2个USB接口。内存64G，硬盘4\*2T，raid5。 交流单电源（可扩展冗余电源），风扇散热。 |
| 性能 | 采集性能 | 10000条每秒单机。 |
| TB级数据秒级检索 | 通过缓存加倒排索引可以对TB级数据进行秒级检索,根据硬件情况最大检索时间在5秒内 |
| 扫描端口数量 | 数量不少于140个，TCP端口100个，UDP端口70个； |
| 搜索性能 | 千万级数据搜索查询延迟小于2秒。 |
| 采集指标 | 工控协议指纹  物联网协议指纹  传统协议指纹  工控设备指纹 | 支持通过kafka,syslog,api等通道进行采集数据 |
| 通过审计IP/MAC自学习、管理平台的资产扫描以及漏洞探针设备进行扫描 |
| 支持HTTP、HTTPS、NetBIOS、SNMP、FTP、Telnet、SSH、MySQL、Oracle、MSSQL 传统协议。 |
| 实时计算与预警CEP | 具有大数据的挖掘分析包括统计、关联与AI建模。包括智能聚合、智能规则报警、复杂事件处理CEP分析、特征库匹配等。 |
| 安全知识库 | 集成专业漏洞库，漏洞知识库82,000+；集成IP归属库、IP信誉度库； |
| 功能指标 | 安全大数据可视化 | 具备工业网络安全的可视分析，包括工控资产的厂商、区域、核心控制等多维分析展示，漏洞、威胁的多维展示，风险评估评分展示。具有不同维度的安全态势可视感知，包括风险态势、威胁态势、资产态势、漏洞态势、攻击态势。 |
| 数据上报 | 态势分析平台平台支持将威胁信息日志、网络行为统计日志、资产信息和主机告警日志数据上报。 |
| 溯源分析 | 支持接收中心侧下发的数据查询指令，并回传对应数据。具体接口标准和功能;支持接收中心侧下发的规则回查指令，根据指令对保存的历史原始流量数据进行回查，并回传对应数据。定时间段内的历史流量趋势，历史数据统计、网络行为日志审计、网络会话日志 |
| 识别协议 | 可识别SMTP,POP3,DNS,NFS SIP、HTTP、HTTPS、MPLS、FTP、SMP、STP、OSINLCP、UDP等1000+通用协议,可识别MODBUS、OPC、S7、IEC 104、IEC 61850、PROFINET、DNP、FINS等20+工控协议 |
| 流量审计 | 提供指定时间、指定 IP、指定 IP 段、指定 IP 对、指定 MAC、指定端口、指定会话、指定协议的统计的总数据包数、总流量数，TCP 同步包数、TCP 同步确认包数 |
| 提供指定时间、指定 IP、指定 IP 段的网络行为日志记录和查询功能，包括：MYSQL 日志、TELNET 日志、FTP 日志、SSH 日志、HTTP 请求日志、HTTP 响应日志、DNS 请求日志、DNS 响应日志、POP3 日志、SMTP 日志、IMAP4 日志、ICMP 日志 |
| 保留网络会话日志，包括 TCP 会话日志和 UDP 会话日志。 |
| 主机行为审计 | 提供主机登录操作信息的记录、查询等功能。包括主机登录系统用户名、登录时间、退出时间、操作命令、操作时间等信息，支持对相关操作行为关联审计及操作路径的回溯。 |
| 设备操作审计 | 态势分析平台提供对各类设备的操作行为的记录、查询等功能。 |
| a）网络设备登录行为审计：应提供网络设备登录信息的记录、查询等功能。登录信息包括登录用户名、登录时间、退出时间、操作命令、操作时间等； |
| b）安全设备登录行为审计：提供安全设备登录信息的记录、查询等功能。登录信息包括登录用户名、登录时间、退出时间、操作内容、操作时间等。 |
| 工控资产拓扑 | 基于工控系统的资产维护，可维护工业控制系统、以及系统关联的工控资产；基于资产的拓扑视图，可以显示资产之间的逻辑连接关系，可在拓扑中动态展示设备运行状态、以及实时流量信息；【提供产品截图证明，报价时以PDF格式上传】 |
| 关联分析 | 支持以事件为中心的关联分析查询，支持事件的IP之间的图计算关联分析，支持IP对应资产、脆弱性的钻取分析、支持事件的聚合分析。 |
| 威胁预测 | 全局威胁趋势预测,可以感知未来某时间或时间段的威胁数量,某类威胁在未来发生概率预测,未知威胁预测,攻击目标预测,攻击来源预测 |
| 统计分析 | 资产统计，以网络资产为中心，分析系统资产相关数据；漏洞统计，以资产关联的漏洞为中心； 事件统计，以网络安全事件为中心，分析事件相关信息。 |
| 安全监测 | 可以通过可疑域名检测、可疑 IP 检测、特征值检测和行为模型等方式对全网流量进行安全监测(内置22类威胁类型) |
| 用户画像 | 基于各种安全事件日志的综合分析，根据攻击源IP地址、攻击类型、攻击工具和方法、攻击时间、攻击目的IP等信息进行综合统计分析，归纳、总结、猜测出用户实时行为,是否进行危险操作、违规行为、攻击意图、潜在风险进行分析 |

**5、主机终端防护参数**

|  |  |
| --- | --- |
| **指标项** | **具体指标要求** |
| 基础要求 | 本次要求提供20点软件授权； |
| 工作模式 | 支持观察模式和执行模式，观察模式只告警、不拦截，执行模式拦截并告警； |
| 系统启动延迟 | 系统开机时间的延迟小于15秒； |
| 系统资源占用 | 系统内存的占用小于20M； |
| 权限划分 | 支持用户权限划分，系统管理员，普通管理员，审计管理员 |
| 操作系统兼容 | 支持Windows操作系统，包括windows Server 2003/2008/2012/2016/2019/Windows 2000/XP/7/8/8.1/10操作系统(32位及64位)以及window7嵌入式英文版； |
| 支持主流Linux系统，包括RedHat5.x、6.x、7.x；CentOS5.x、6.x、7.x； |
| 白名单管理 | 支持白名单库的导出备份及导入； 支持对白名单进行关键内容、模糊查询查找； 支持对白名单库进行追加、删除、保存等自定义操作； 支持白名单网络化管理 |
| 系统固化 | 支持对系统进行一键固化操作，自动生成白名单库； |
| 白名单防护 | 支持程序或进程、脚本的白名单防护，禁止白名单以外的非法进程或脚本运行，并产生安全告警事件；  支持配置白名单防护模式为观察模式或执行模式，观察模式下只告警不拦截，执行模式下拦截且告警； 支持将告警的程序一键添加到白名单； |
| 白名单更新 | 支持对手动安装的软件进行自动追踪并添加到白名单列表中；  支持基于目录或文件对绿色软件追加； |
| 完整性保护 | 支持对应用程序、操作系统的完整性检查防护，阻止病毒、恶意软件的篡改和破坏 |
| 信任管理 | ★支持自定义添加或删除信任的文件或目录，信任路径内程序执行不会被拦截 |
| ★支持添加或删除信任的可执行程序，并对信任程序在运行过程中动态释放和加载非白名单中的程序或文件自动加载到白名单中 |
| 进程运行记录 | 支持对进程启动或停止的记录； |
| 移动存储管理 | 支持对普通U盘的访问控制，包括只读、只写、执行； |
| 支持基于白名单的U盘接入管理，支持对单一Ｕ盘的独立权限控制，杜绝一切非注册U盘接入； |
| 支持安全专用U盘的注册、认证、授权，支持读写权限管理； |
| 完整性保护 | 对特定安装目录的文件进行完整性保护，防止恶意程序篡改或误操作对目标文件进行修改或删除； |
| 安全加固 | 支持对特定注册表进行防篡改保护 |
| 支持对关键业务进程进行防杀保护； |
| 支持对操作系统的审核策略、安全选项等进行统一的设置； |
| 自身防护 | ★支持软件自身防护，防止非授权结束进程，禁止程序文件被删除，降低安全风险 |
| 支持白名单策略文件被删除或篡改； |
| 安全审计 | 支持对白名单策略外的程序警报、U盘警报、外设警报、保护警报等各类安全告警审计及其统计分析； |
| 支持对系统的程序日志、USB日志、进程运行日志、设备接入日志、操作日志等进行统计记录，并可进行查看； |
| 支持对日志进行备份、还原管理； |
| 参数配置 | 支持对系统的状态进行设置，包括白名单防护模式、报警方式、自身防护状态等； |
| 资质要求 | ★投标产品应具有公安部计算机信息系统安全专用产品《销售许可证》； |
| ★投标产品应具有中华人民共和国国家版权局《计算机软件著作权登记证书》 |

**6、工业防火墙（1U）**

|  |  |
| --- | --- |
| **指标项** | **指标规格要求** |
| 硬件要求 | 配置至少6个10/100/1000M速率RJ45业务端口；可以扩展光口， RJ45接口支持内置Bypass，至少支持3对BYPASS，支持断电Bypass和软件“看门狗”； |
| 配置1个带外RJ45 MGT网络管理端口； |
| 平均无故障时间MTBF(小时)要求高达200000h。 |
| 硬盘容量不小64G； |
| 性能要求 | 网络吞吐量4Gbps，并发连接数300万，新建连接数8万。DPI吞吐量2G。； |
| 工作模式 | 支持告警模式、防护模式 |
| 部署模式 | 支持透明模式/路由模式/混合模式 |
| 管理模式 | 支持自管理部署，集中管理部署 |
| 事件信息 | ★支持策略安全事件（包括黑名单、白名单、IPMAC、会话连接事件）、规约告警事件、系统事件告警或记录。 |
| 支持策略安全事件、规约告警事件、系统事件统计，规约告警事件统计分析，提供图形可视化的展示分析功能 |
| 支持从安全事件跳转至对应的安全策略 |
| 支持系统本身所发生的事件，例如:添加/删除规则，及设备端口状态等 |
| 支持页面流量记录中，包括设备名称、IP 地址、MAC 地址、平均输入速率（1 小时）、平均输出速率（1 小时）、平均流量百分比、更新时间。点击流量记录中“详情”按钮，可查看设备流量信息。包括实时流量，最近 1 小时、1 天、1 周的协议流量占比，该设备不同时间下的流量协议名、平均流量百分比。 |
| 基础防火墙功能 | 支持包过滤、应用状态检测防火墙功能。 支持对网络报文进行过滤和控制，支持基于MAC地址，IP地址，协议，端口号，时间段等访问控制策略。 |
| 支持自学习 在页面上方学习区域内，选择“学习时长”，5 分钟，30分钟，1小时，2小时，10小时，16小时，1天，3天， 1 周时间自由设置。 |
| NAT | 支持源地址NAT和目的地址NAT。 |
| VPN | 支持IPSEC VPN功能 |
| 白名单防护 | ★支持工控协议的深度解析功能，支持基于机器学习方式自动记录并梳理工控协议中的操作行为规律，并通过这些行为和规则逐步形成白名单防护规则，支持规则的处理动作批量配置。 |
| 支持工控协议自定义规则并形成安全策略，对不符合安全策略的数据包进行阻断或报警，并产生告警信息。 |
| 工业协议支持 | ★支持工控协议的深度解析不少于20种（包括但不限于OPC Classic，OPC UA,Modbus TCP，Modbus UDP，Siemens S7，Ethernet/IP(CIP)，IEC104，DNP3，MMS，Profinet,PNRTDCP,GOOSE,SV,ENIPTCP，ENIPUDP,BacNet，853，Omron Fins等。 |
| 黑名单规则 | 工控威胁漏洞库至少达到1200条。 |
| IPMAC绑定 | 支持IPMAC绑定，可以根据网络流量主动学习IPMAC地址，也可以主动添加IPMAC地址组，防止IP地址盗用，对未知接入设备进行监控，告警或者阻断。 |
| 自定义协议 | ★支持用户通过协议特征的方式添加新的协议，并可以对新添加的协议进行识别，规则匹配，产生相关安全事件。 |
| 安全策略日志 | ★支持基础防火墙、白名单、连接管理等产生的日志，记录基于时间、源IP、源MAC地址、源端口、目标IP、目标MAC地址、目标端口、协议类型等的行为和内容，并提供过滤查看和导出功能 |
| 拓扑管理 | ★内置工控设备指纹库，能够自动识别防火墙所在的网络节点位置处的所有连接的设备，并以拓扑图方式展示出来 |
| 设备管理 | 支持自管理，可对设备、用户、接口等进行配置管理， |
| 提供直观的接口配置页面，支持对端口信息、端口模式及静态路由信息进行修改配置 |
| 支持对当前设备的系统强制登出时间、用户可尝试登录次数进行灵活设置 |
| 提供Syslog远程服务配置，配置完成后，可用户可以通过syslog协议，将日志信息以数据报协议(TCP或UDP)方式传送到远端syslog服务器。 |
| 安全防护 | 支持通过配置开启自身的安全防护，支持安全区域的DDOS攻击防护，包括SYN、UDP、ICMP等Flood攻击防护；支持TearDrop、LAND、WinNuke等攻击防护；支持端口扫描攻击防护，包括针对TCP端口和UDP端口的扫描攻击； |
| 产品资质 | ★计算机信息系统安全专用产品销售许可证 |
| ★计算机软件著作权登记证书 |

**7、安全隔离与信息交换系统参数**

|  |  |
| --- | --- |
| **指标项** | **具体指标要求** |
| 系统架构 | 1、采用2+1系统架构即内网单元+外网单元+专用隔离硬件。不能采用网线等形式直通。  2、采用基于linux内核的多核多线程专用安全操作系统，加固内核。 |
| 硬件要求 | 2U标准机架式、4个10/100/1000Mbps自适应电口 |
| 管理接口 | 外网端不允许配置任何形式的管理接口，所有管理配置操作均通过专用的网闸内网可信端管理接口进行配置。 |
| 部署模式 | 设备支持透明、代理及路由三种工作模式，管理员可依据实际网络状况进行相应的部署。 |
| 内置应用 | 产品内置各类应用支持模块，无须用户增加投资，功能模块至少包含：邮件模块、安全浏览模块、视频交换模块、数据库访问模块、数据库同步模块、文件交换模块、OPC模块、MODBUS模块、WINCC模块、组播代理模块、用户自定义应用模块等各类应用模块,并可控制相应应用协议的的动作、参数、内容。 |
| 文件交换 | 支持Samba、FTP等多种文件协议，可以实现内网到外网、外网到内网、双向的文件传送。 |
| 支持病毒检测 |
| 支持对文件类型的黑白名单控制，根据文件格式特征进行过滤，并且不依赖于文件扩展名；  支持文件内容深度检测，对包含关键字内容的文件进行过滤 |
| 支持增量传输、传输后删除等传输策略；  支持目录内子目录同步，子目录级别不受限制； |
| 支持文件交换容错和告警功能，交换出错能够自动重传，出现异常能够告警提示并记录日志； |
| 可通过专用客户端或共享方式提供安全的文件同步功能 |
| 数据库同步 | ★支持Oracle、SQLServer、Mysql、Sybase、DB2、Postgresql等多种主流国外数据库的同步和国产达梦数据库、人大金仓数据库的同步 |
| 支持同构、异构数据库之间的同步，如Mysql同步至Oracle。 |
| 支持字段级数据同步，仅同步表中某几个字段。 |
| 支持BLOB、CLOB等大字段的同步。 |
| 同步功能由网闸主动发起并完成，无需在数据库安装方软件，支持Windows、Linux、Unix 等多种数据库操作系统，且网闸无需开放端口以杜绝安全隐患； |
| 同时支持客户端方式，提供更高性能的数据库同步。 |
| 支持数据库同步实时日志记录，提供日志审计、查询 |
| 数据库访问 | 支持Oracle 、DB2、SyBase、SQL Server、MySql等主流数据库的安全访问，实现内外网之间数据库及表内容安全传输。 |
| ★支持SQL语句控制，如只允许查询，不允许删除等 |
| 支持任务单独启停管理，不影响数据库同步的其他任务运行。 |
| 支持对访问源地址、目的地址、本机地址和端口的自定义访问控制。 |
| 安全浏览 | 支持应用层指令控制，如GET、POST、PUT、HEAD、CONNECT、等。 |
| 可限制用户行为，如只允许浏览不允许登陆等 |
| 支持代理模式 |
| 支持URL地址过滤，并可限制网页中的Script脚本、ActiveX脚本、java applet等 |
| 支持关键字网页过滤；支持对下载文件的大小、类型过滤； |
| 邮件交换 | 支持SMTP、POP3协议；支持病毒检测功。 |
| 支持邮件地址、附件、主题、内容等进行过滤。 |
| 支持附件大小、附件格式控制；支持发件人、收件人过滤。 |
| TCP应用传输 | 支持TCP应用层数据单向传输的控制，保证TCP应用数据的0 反馈，以满足二次防护对数据传输的安全性需求。 |
| 组播代理 | ★系统支持多任务的组播代理功能，可穿透三层交换机网络进行部署，支持PIM协议 |
| 工控通讯协议 | 支持OPC、Moudbus、DNP3、IEC61850\_MMS、IEC104、S7等工业控制协议 |
| 工业控制应用 | ★支持OPC协议。支持同步、异步监测数据的传输，只需绑定固定的一个起始端口即可满足动态端口的数据传输。可控制功能代码，比如只允许读取，不能写入等 |
| ★支持MODBUS协议，可按照用户需求控制具体功能代码，比如控制线圈、值域范围等 |
| ★支持西门子的WINCC控制协议，可按照用户需求控制功能代码，比如只允许读取，不能控制等 |
| 自定义应用 | 支持自定义的TCP、UDP协议的数据隔离交换，以用户定制的命令、参数等来限定隔离通道内的数据内容。 |
| 管理用户 | 符合国家标准，采用三权分立设计。系统策略配置管理员、安全管理员与日志管理员三种角色，各用户只能维护操作本类管理功能与操作。 |
| 诊断工具 | 系统提供ping、traceroute 、TCP端口探测、抓包等工具，方便管理员在配置策略或调整网络时排查问题。 |
| 安全管理 | 支持HTTPS的Web方式管理，可实时监控CPU、内存、硬盘、网络流量等状态；实现了远程管理信息加密传输；支持命令行方式管理，可以通过命令方式进行资源分配、排错、查看日志、深层次管理。 |
| 日志审计 | 系统可存储和审计包含：系统日志；管理日志；网络活动日志；入侵报警及处理日志；访问控制日志。 |
| 双机热备 | 支持双机热备及多机热备功能，最大化的保障业务可用性。  支持配置同步，通过独立的热备端口实现双机热备。 |
| 资质证书 | 1. 公安部计算机信息系统安全专用产品销售许可证；  2. 计算机软件著作权证书； |

**8、工控安全审计系统参数**

|  |  |  |
| --- | --- | --- |
| **指标项** | **技术规格要求** | |
| 硬件指标 | 标准机架式安装 | |
| 至少配备4个千兆电口、1个管理口。最大可扩展为20个千兆电口 | |
| 工作温度：-40℃～85℃，防护等级≥IP20； | |
| 性能指标 | 能够自定义审计数据的存储位置 | |
| 网络安全日志留存的时长不少于六个月 | |
| 软件功能 | 部署模式 | 旁路工作模式 |
| 管理模式 | 支持自管理部署，集中管理部署 |
| 安全事件 | 支持策略安全事件（包括黑名单、白名单、IPMAC、会话连接事件）、规约告警事件、系统事件告警或记录。  支持策略安全事件、规约告警事件、系统事件统计，关键事件统计分析，提供图形可视化的展示分析功能 |
| 能够显示系统本身所发生的事件，例如:添加/删除规则，及设备端口状态等 |
| 支持规约告记录警功能，即能对网络流量中不符合协议规约数据包进行告警记录。 |
| 支持关键事件告警记录功能：即能对对工控系统中一些关键操作的指令进行识别并进行告警记录。 |
| 能够显示当前工控系统中触发安全规则所所产生的安全事件信息。 |
| 会话审计 | ★支持对网络数据报文基于IP地址，协议，端口号等元素的会话安全审计  ★支持登录日志记录了用户的登录操作，点击“过滤条件”可以根据开始 时间、结束时间、ip、登录状态、用户、原因来对登录日志进行过滤查看。 |
| 工控协议白名单审计 | 支持工控协议的深度解析功能，支持基于机器学习方式自动记录并梳理工控协议中的操作行为规律，并通过这些行为和规则逐步形成白名单防护规则，支持规则的处理动作批量配置。 |
| 支持工控协议自定义规则并形成安全策略，对不符合安全策略的数据包进行报警。 |
| 工业协议支持 | 支持工控协议的深度解析不少于20种（包括但不限于OPC Classic，OPC UA,Modbus TCP，Modbus UDP，Siemens S7，Ethernet/IP(CIP)，IEC104，DNP3，MMS，Profinet,PNRTDCP,GOOSE,SV,ENIPTC P，ENIPUDP,BacNet，853，Omron Fins |
| 支持对工控协议的指令级审计，能够对应用层报报文字段类型、功能码、数据内容进行解析。 |
| 工控威胁特征库 | 内置威胁特征库不少于1200个，对网络中的入侵攻击进行实时告警及记录 |
| 未知设备接入检测 | ★根据网络流量主动学习IPMAC地址，也可以主动添加IPMAC地址组，检测IP地址是否被盗用，对未知接入设备进行监控告警【提供功能截图，报价时以PDF格式上传】 |
| 协议分析 | 支持对监测到的数据进行实时分析，显示源IP地址、源MAC地址、源端口、目的IP地址、目的MAC地址、目的端口、抓取时间、协议类型及对其搜索，支持协议要包含http、ftp、pop3、smtp、telnet、snmp、OPC Classic，OPC UA,Modbus TCP，Modbus UDP，Siemens S7，Ethernet/IP(CIP)，IEC104，DNP3，MMS，Profinet,PNRTDCP,GOOSE,SV,ENIPTCP，ENIPUDP,BacNet，853，Omron Fins等。可以查看监测数据的PDU类型、操作类型、数据类型等。 |
| 无流量监测 | ★支持对opcda、iec104等工控协议的无流量监控，并支持无流量认定时长的设置。支持无流量监控行为告警记录【提供功能截图，报价时以PDF格式上传】 |
| 流量分析 | 支持对流量数据长期的统计分析，包括总流量的统计以及设备流量和协议流量占比统计，并以图形可视化的方式进行显示，支持以小时、天、星期过滤。流量列表中体现设备名称、IP地址、MAC地址、平均输入输出速率、更新时间和具体操作。 |
| 支持对工控网络进行实时监测，对协议、流量等元素进行统计分析，实时显示网络的状态 |
| 数据采集 | ★支持对原始数据包的采集，要针对网口、pcap包大小、协议号、源IP地址、目的IP地址、源端口、目的端口好进行针对性采集。支持数据包批量下载删除操作。 |
| 系统安全性 | 安全性要求，产品自身安全性强，硬件加固，软件加固，数据加密，杜绝泄密源，自身认证授权功能严格加强。 |
| 产品资质 | 具有中华人民共和国国家版权局《计算机软件著作权登记证书》【提供有效证书复印，报价时以PDF格式上传】  具有公安部计算机信息系统安全专用产品《销售许可证》【提供有效证书复印，报价时以PDF格式上传】 | |

**备注：**

1、上述打“★”项为重要指标项，必须完全实质性响应；其他项参数在不影响产品的功能特点和整体结构的基础上，允许适度偏离，但必须与询价文件所述相一致，偏离是否适度、是否科学合理，将由评委给予综合评价，供应商应承担被判定为偏离度过大，已影响产品功能特点和整体结构，报价无效的风险。

2、签订合同后，需提供样机进行上述功能要求的逐一测试验证。如有虚假响应，供应商须承担相应责任。

3、以上采购要求中如涉及产品品牌或型号，是采购人根据项目所要实现的功能推荐的品牌或型号，并不是限制条件，供应商可以采用不低于推荐的产品档次设计方案并参与竞争。但是，所有产品的质量、技术参数和功能以及方案品质不得低于采购要求，并确保整体性能的合理以及能最终实现。（若非推荐品牌或型号，供应商必须提供必要的证明材料。询价小组根据其相关证明材料判定是否达到所推荐的产品档次等要求。）

4、为保障江南水务安全防护效果，打造江南水务整体安全运营体系，要求本次项目供应商提供的产品必须与江南水务现有安全体系能够兼容对接，保障一体化安全体系防护，不得出现无法兼容的情况。

**四、项目实施要求**

**1、项目管理要求**

（1）成交供应商必须接受并服从采购方的监督、管理要求。无条件接受采购方提出的整改要求，并承担相应责任。

（2）成交供应商在实施过程中应加强施工管理，特别对采购方提出的问题应在约定的时间内及时解决，并提交书面报告，否则由此导致的延迟责任由成交供应商承担。

（3）成交供应商须按采购方所规定的时间将设备安装到位并调试运行。成交供应商在项目实施过程中出现资源、进度、质量协调控制不力并影响到项目工期的，采购方有权与供应商终止合同，供应商并须承担相应责任。

**2、项目保密要求**

供应商必须承诺对实施过程中的文档、资料、数据均有保密义务，由于成交供应商及其实施人员泄露、冒用、误用或违法使用而造成的一切责任和损失，均由成交供应商承担。

**五、保修期及售后服务**

1.提供3年原厂质保服务及我公司项目整体免费上门质保服务，在免费保修期内发生故障，成交供应商应免费提供咨询、更换损坏的零件和维修服务。

2.为保障项目稳定运行，成交供应商须负责相关设施故障或损坏后的修复，使相关设备设施无告警和异常，保持安全、稳定、高效运行。每月不少于一次预防性检查和维护。

3.出现故障接通知后10分钟内响应，需在1小时内到达到现场；提供7X24小时现场服务，备件24小时到位；一般问题到达现场后2小时内解决，所有问题解决时间不得超过24小时。

4.质保期内维护设备、配件、设施和服务不再收取任何其他相关费用，如配件费、维修费、劳务费、交通费、培训费等。

**六、项目完工期限**

签订合同后60个自然日内。

**七、完工地点**

采购单位指定

**八、付款方式**

合同签订后付款50%，项目竣工验收合格后付款40%，验收合格满一年后支付10%尾款。

**九、其他相关要求**

1.项目实施过程中所需的采购文件中未列出的相关辅助材料和费用应由供应商在报价时一并考虑，项目施工过程中不再单独结算。

2.本次项目供应商严格按照等保2.0要求，对本次项目进行充分调研分析，结合江南水务集团系统架构及系统实际情况，制定详细合理的方案、完成整个项目的实施工作，必须确保项目通过等保2.0测评。

3.本次项目用于江南水务集团平台，必须充分结合该平台系统架构及系统实际情况，在部署实施后不能对集团平台上的系统业务产生影响、降低性能。如果产生影响，成交供应商进行相应整改，费用由成交供应商负责承担。

4.项目完成后，根据采购人要求组织验收，相关费用由成交供应商承担。

5.供应商可对现场进行勘查（不统一组织、因供应商不进行现场勘查造成辅材附件费用计算不准等的后果均由供应商负责，现场勘查联系人及电话：刘先生0510-88011005 ）。