# 关于网络安全设备的网超采购调研公示

**第一部分 须知前附表**

|  |  |
| --- | --- |
| **序号** | **主　　　要　　　 内　　　 容** |
| 1 | 调研报名公示开始时间： 2021年  6 月　25　日上午10点30分北京时间  调研报名截止时间：2021年　7 月　1　日下午17点30分北京时间  (加盖公章的项目文件回执单、报名条件、报名材料、网超截图、公司证件)  调研会时间：2021年7 月2日上午9点北京时间 |
| 2 | 项目：关于网络安全设备的网超采购调研公示 |
| 3 | 文件正本　 1　份，副本　 4　份。 |
| 4 | 文件递交处：　福建省肿瘤医院 网络办会议室 |
| 5 | 上述时间、地点如有变动，以单位届时通知为准。 |

**地　址： 福建省福州市福马路420号省肿瘤医院科研楼四楼网络办**

**邮　编： 350001**

**电　话： 0591-83660063-8822**

**联系人：钱工**

随着医院信息化建设的发展，加强等保2.0下的网络安全，同时满足医院业务增长的需要和网络的安全稳定运行，本次拟在网超采购下述设备：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 设备规格 | 主要参数 | 数量 |
| 1 | 安全审计系统 | 1. 软硬件一体化产品，2U、硬盘1T\*2、硬盘须配置RAID1、至少配备6个100/1000M自适应电口、4个1000M光口（含2个SFP多模模块），1+1冗余电源， 2. 可管理设备数量≥500个，运维用户无限制，单台堡垒机字符类并发会话≥500、图形类并发会话≥100 3. 支持集群部署模式，中心采用HA，节点可以横向扩展，实现统一登录入口、统一配置同步、审计日志集中查询、实时会话集中监控，以满足业务增长需求。 4. 支持按部门组织架构（至少5个层级的部门）管理用户数据、资产数据、授权数据、审计数据 5. 每个部门可以管理本部门及下级部门的用户角色：部门管理员、运维管理员、审计管理员、运维员 6. 每个部门的审计管理员可以管理本部门及下级部门的运维会话日志 7. 产品内置VPN模块，无需与其他VPN设备联动，实现运维入口安全接入 8. 支持与get、post、soap发送方式的http短信网关平台进行联动，实现短信动态口令双因素认证机制，如与阿里云短信服务、SendCloud联动 9. 支持手机APP动态口令认证方式登录堡垒机，且新用户首次登录后需强制绑定APP动态口令 10. 支持基于国密算法的动态令牌进行双因子认证，支持采用国密加密算法进行核心敏感数据加密存储 11. 支持认证窗口的全局设置：可以选择启用哪种或者哪几种认证登录窗口 12. 支持DB2、oracle、mysql、sqlserver主流数据库协议代理运维，可直接调用本地windows系统的数据库客户端工具，支持自动登录、无需应用发布前置机 | 1 |
| 2 | 安全审计系统 | 实现交换机及服务器综合日志审计。（等保2.0要求）  2U标准机架，标准配置6个千兆电口、4个SFP接口、2个扩展槽；整机最大可以支持26个千兆接口；2个USB口，1个控制口，6T企业级硬盘。  对大量分散设备的异构日志进行统一管理、集中存储、统计分析、快速查询，实现即时告警，满足IT安全要求。  1）支持Syslog、SNMP Trap、文件导入、WMI、SMB、数据库等日志采集方式。内置不少于200种设备的日志解析规则；  2）支持日志采集过滤，减少日志采集量；  3）支持日志归并功能，对采集到的重复的日志进行自动的聚合归并。日志源授权点数：200点；日志处理性能≥30G/天；  4）支持与现有安全感知与运营管理平台联动，实现日志统一集中平台管理。  5）支持拓扑管理功能，可根据资产生成拓扑，并可通过拓扑查看资产事件、告警等。  6）支持日志采集过滤，可配置过滤策略，根据设备名、类别、级别、IP、端口、MAC、动作等组合条件进行过滤，减少日志采集量。  7）支持日志归并功能，对收集到的重复的日志进行自动的聚合归并，减少日志量。  8）系统全面支持IPV6,可审计IPV6设备日志。 | 1 |
| 3 | 防火墙 | 实现下一代防火墙设备冗余。（等保2.0要求）  1U标准机架式设备，标配6个千兆电口，2个扩展槽，2个USB口,1个COM口，1T硬盘； 含三年IPS、AV、应用识别特征库升级服务。最大吞吐量≥5Gbps，并发会话≥120万，新建会话≥4万，IPS吞吐量≥800Mbps，防病毒吞吐量≥800Mbps  1)具有应用安全防护、抗攻击、应用可视化、VPN、智能流控、恶意内容过滤等功能。  2)提供网络边界区数据过滤、文件过滤、流量管理以及各种网络安全威胁的保护。  3)支持路由、网桥、单臂、虚拟网线以及混合部署方式；  4)支持与现有安全感知与运营管理平台联动，实现自动封堵策略。  5）支持用户和用户组管理，支持批量添加用户，支持对不同用户配置不同的安全策略，包括访问控制、应用控制、入侵防护、病毒防护等安全策略；  6）支持网络资源分级管控，根据不同的资源等级分配不同的安全控制级别，只允许具有相应级别权限的用户访问；  7）支持抵御网站扫描、SQL注入、XSS、命令注入、CSRF、远程代码执行、JAVA反序列化、文件上传、目录跳转、WebsShell上传等Web应用攻击；  8）支持Land、Smurf、WinNuke、Ping of Death、Tear Drop、IP地址欺骗攻击防护，支持SYN Flood、UDP Flood、ICMP Flood、DNS Query Flood攻击防护，支持IP地址扫描和端口扫描攻击防护，支持异常报文攻击检测；  9）支持对网站的恶意扫描防护和恶意爬虫攻击防护；支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等；  10）支持针对网站的漏洞扫描进行防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测；  11）支持查看当前所有配置和规则信息，支持按功能模块进行策略配置备份和恢复；  12）支持与现网态势感知联动，实现日志统一平台管理。 | 2 |
| 4 | 多网隔离系统 | 实现安全接入医院网络（等保2.0要求）  2U标准机架，标配4个1000M电口和3个扩展槽；含100个PC客户端网络接入授权；  1、 支持配置多个网桥，支持配置网桥IP，网桥模式部署时支持VLAN、PPPOE和策略路由。  2、 支持链路聚合支持PPPoE接入，支持ARP代理，VLAN子接、口、VLAN、Trunk、802.3ad、STP；  3、 支持多个业务网络的接入，接入的计算机或移动终端无需重启系统或注销已登陆的业务网络，在同一操作页面一键自由切换不同业务网络；并且同一时刻，接入的计算机或移动终端能且只能访问一个业务网络，即登陆某个业务网络时，无法访问其他业务网络。  4、 内置定义了外网和内网两个业务网络，当PC访问外网时，数据存储在加密的外网分区，当PC访问内网时，无法访问PC的外网分区文件，从而禁止外网下载的可疑文件内网运行。 | 1 |
| 5 | 网络入侵检测系统 | 实现网络入侵检测。（等保2.0要求）  2U标准机架式设备，模块化设计，标配6个千兆电口，2个万兆SFP接口，配2个万兆单模模块，2个扩展槽；2个USB口，1个COM口，128G SSD固态盘，4T企业级硬盘；每秒TCP新建连接数≥18万，最大TCP并发会话数≥200万，整机吞吐率≥10Gbps，IDS吞吐率≥5Gbps。对网络传输进行即时监视，在发现可疑传输时发出告警或者采取主动反应措施，阻止网络攻击。具备以下特征：  1)展示恶意外联趋势、总数、活跃域名统计 、源ip、关系图等信息；  2)展示扫描探测趋势、总数、源IP、目的IP详细信息；  3)展示Web攻击趋势、总数、详情及统计等数据；  4)支持与现有态势感知联动；  5）展示选定时间内的文件检测威胁趋势、危险文件总数、危险文件下载源IP Top10、危险文件下载目标IP Top10、病毒文件类型、文件关联邮箱、文件关联URL、文件报告列表，提供病毒文件样本下载功能；  6）展示选定时间内的扫描探测趋势、扫描探测总数、扫描探测源IP Top10、扫描探测目的IP Top10、扫描探测详细信息；  7）支持通过E-mail邮件、SNMP Trap、Syslog、Windows消息框、短信、FTP等方式告警；支持与态势感知形成联动。  8）针对证据库的任意查询结果，系统能立即自动统计分析。统计信息包括：总记录数、源IP统计数、目标IP统计数、查询事件数、源IP各级别统计TOP10、目标IP各级别统计TOP10、证据分类、各级别危险统计TOP10；  9）事件详情查看中以分类规整方式动态嵌入与之相关的攻击证据，并能实现证据内容的无限次数的钻取。分类方式应包括：尝试获取用户信息、疑似敏感行为、尝试获取用户权限、疑似Web应用攻击、疑似木马活动、病毒扫描、协议异常、网络扫描、异常连接；  10）内置攻击检测引擎和攻击检测规则库，攻击关联分析引擎，可准确网络中的异常行为，并通过攻击行为专家识别系统，将多个攻击告警关联成一个安全事件； | 1 |
| 6 | 安全感知与运营管理平台 | 对攻击、威胁和合规三大态势进行安全事件数据感知，实现告警及安全联动。  2U标准机架式设备，全模块化设计，标配6个千兆电口，4个千兆SFP接口，3个网络扩展槽，2块6T硬盘，2个USB接口，1个COM口；配置350个监控节点授权；冗余电源；  含资产发现、漏洞扫描、日志采集、工单管理、多源日志关联分析、可视化大屏等功能。安全事件采集能力≥6000 EPS；≥140亿条日志存储能力；含3年硬件维保服务，含3年威胁情报库升级服务授权。  资产发现与管理、漏洞扫描与管理、资产风险分析、IP画像、告警事件采集、关联分析、态势分析展示；支持对网络设备、安全设备、操作系统、应用中间件日志的深度解析和范式化处理；  持通过Syslog、SNMP Trap、FTP、Web API、Kafka、NetFlow等方式采集数据；与现有防火墙系统安全联动，实现网络安全运维自动告警、自动阻断封堵。   1. 支持大屏展示综合态势，从资产、漏洞、攻击、告警等维度呈现整体安全状态，包括安全评级、资产总数、漏洞分布、漏洞top5、高危漏洞、告警总数、已封堵ip、安全事件趋势等信息; 2. 支持大屏展示攻击态势，包括攻击目标系统排名TOP5、重点系统攻击情况、攻击类型top5，并支持攻击全景地图展示; 3. 支持的日志采集方式包括但不限于：Syslog、SNMP Trap、Kafka、Web API接口、FTP、Netflow、agent等方式采集日志，提供日志采集方式界面 4. 支持采集的设备类型：路由器、交换机、防火墙、IDS/IPS、WAF应用防火墙、APT威胁检测防御设备、数据库审计、网络审计、堡垒机、主机监控系统、安全扫描设备、网页防篡改系统、Windows、Linux、Unix、Apache、IIS、JBoss、Tomcat、Nginx、WebLogic、牙木DNS等; 5. 支持日志的备份和恢复。支持通过等SSHFS、NFS等协议备份日志数据; 6. 资产审核：支持资产的审核管理，与资产自动引擎识别等资产进行审核与信息不全，实现资产自动发现、资产审核以及资产入库管理的资产全生命周期管理； 7. 工单管理：支持漏洞、告警的派单处理，按照安全运维的设定流程进行工单流转并最终到达该告警的负责人，该负责人进行告警事件的处理，在处理过程中，该工作单的处理过程的各个状态可查看、可追踪。 | 1 |
| 7 | 云主机入侵风险感知 | 采集互联网安全事件数据，实现风险告警。  1、监控服务器主机安全配置变更状态，包括：身份鉴别、访问控制、安全审计、剩余信息保护等方面，一旦监控配置发生变更，能及时产生相关的告警。  2、对服务器主机系统的进程、网络连接、异常DNS请求、可疑后门等进行安全监测，结合内置威胁情报，及时发现恶意IP与恶意域名。  3、在主机监控页面上能实时直观展现资产信息、告警趋势、监控详情、系统配置监控、采集记录情况。风险感知展示详细资产信息包含：分组、IP地址/MAC、主机代号、资产名称、主机名、操作系统、最近通信时间等 | 1 |

为保障网络稳定性与兼容性，本次预算调研设备品牌为安恒、启明星辰、黑盾。

欢迎有意向的供应商等参与本次调研。

调研说明：

1. 本次报名截止时间为2021年7 月1日下午17点30分北京时间；
2. 调研会时间：2021年7 月2日上午9点北京时间；
3. 报名时需提供（加盖公章的项目文件回执单、报名条件、报名材料、网超截图、公司证件）；
4. 本项目实施主要工作为：上述各设备安装调试、上架、设备集成等硬件安装工作，同时必须结合医院现有网络安全设备拓扑，实施网络安全规划、等保安全配置等各项工作；
5. 参加公司应准备PPT材料（含产品介绍、网超价格、服务及集成能力、应用案例等），文件正本1份，副本4份，每公司讲解时间30分钟；
6. 欢迎供应商前来参与，每一品牌限前1名报名。

**项目文件回执单**

**请各公司在一周内将此项目文件回执单送到“福建省肿瘤医院网络办”。**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **公司名称** | **产品名称** | **报价** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |

**公司名称：**

**联系人：**

**联系电话：**

**邮箱号：**

**公司盖章：**

**2021年　月　日**