第五章　　采购需求

1. 项目背景

通过本项目的开展,不断提升首都医科大学附属北京安定医院(以下简称“安定医院”）网络及信息系统的安全性，降低系统信息安全事件发生的概率，减少信息系统中断风险，保证业务系统的高可用性，提升业务工作效率，不断完善业务和信息资源的管理。

2. 本次采购的产品

序号	名称	数量	单位
1	防统方	1	台
2	内网应用域防火墙（核心产品）	2	台
3	外网核心交换机	2	台
4	外网业务域防火墙	2	台

3. 技术参数要求

3.1. 防统方

序号	技术指标	详细技术参数
1.	硬件规格及性能	采用独立的标准机架式 2U 硬件架构，软硬件一体化系统，全操作系统，内嵌数据库，用户无需另外安装操作系统及数据库管理系统。
2.		内存≥16GB;≥6*100/1000M 电口;硬盘存储≥2TB,采用 SSD、HDD 多级存储架构，系统和业务数据分离，实现高效、安全存储；
3.		性能指标：峰值事件处理能力不低于 25000 条语句/秒，日志存储不低于 16 亿条。
4.	工作模式	旁路部署方式，对原有网络不造成影响，产品本身的故障不影响被审计系统的正常运行,不得在现有服务器上安装可能带来风险的程序。
5.		支持 Agent 引流，运行时 CPU 占用率低于 3%，内存占用小于 100M，程序文件小于 5M。

6.		支持分布式部署方式，并支持集中管理功能，可快速查看所有防统方系统的状态、风险状态等；（提供截图并加盖投标人公章）
7.	基本功能	支持 oracle、SQL Server、Mysql、DB2、Kingbase、神通、南大通用等数据库的审计，且支持多种不同的数据库同时审计。
8.		#系统支持杭创、键讯、金蝶慧通、用友、中联、阳光用药、天健、厦门智业、科进、中天、天网、方正、东华、金仕达、东软、键讯、陕西医星、长城、广州力锦等 his 中间件审计。（提供截图并加盖投标人公章）
9.		系统包括审计引擎及管理后台软件、策略管理、告警管理、权限管理、系统日志、系统配置等功能，审计数据统一存储、查询、分析、统计。
10.		系统内置有多级缓存机制，能够实现超出总容量的 30%时支持时间不低于 2 小时，有多级物理存贮机制；
11.		系统应支持多层过滤功能，支持网络流量驱动级过滤，根据过滤的条件（如源地址 IP/目的地址 IP）定义规则，对网络流量进行扫描，对无用的信息从网络层进行过滤；根据系统语句（SQL 语句）和白名单（条件为 IP/MAC/数据库账户/审计对象/操作语句）定义规则进行应用层过滤，将客户关注的信息进行保留，避免无用信息的堆砌造成磁盘空间的浪费和性能的耗损；
12.	防统方审计能力	#全面支持后关系型数据库 Cache 的集成工具 Terminal、Portal、Studio、Sqlmanager、MedTrak 工具的审计，其中 Portal 能审计到 Sql 语句、查询 Global 有返回结果，Sqlmanager 支持根据 SQL ID 提取高效审计， Terminal 能审计到 SQL 语句和返回结果,并支持本地审计，基于 C/S 的 MedTrak 工具能审计到操作报表的具体返回结果；（提供截图并加盖投标人公章）

13.		支持超长操作语句审计，针对传统型数据库，支持 3 万字节审计而不截断；
14.		支持对执行时间超过 6 小时操作的审计。
15.	应用审计能力	#支持 B/S、C/S 应用系统三层架构 http 应用审计，可提取包括应用系统的人员工号（账号）在内的“六元组”身份信息，精确定位到人，并可获取 XML 返回结果；（提供截图并加盖投标人公章）
16.		支持带 COM、COM+、DCOM 组件的三层架构应用审计，可提取包括应用层工号（账号）之内的“六元组”身份信息，精确定位到人；
17.	防统方策略支持	系统自带各种常见 HIS 防统方规则库，且规则数量≥500 条以上，支持自定义防统方规则；
18.		#支持统方确认，点击查看某条审计记录，能够进行统方确认，此时该条审计记录就会从审计记录中移除，加入到统方报表中。（提供截图并加盖投标人公章）
19.		防统方策略支持 18 种以上审计元素，可支持数据库操作命令、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端 MAC、客户端 IP、客户端端口、客户端进程名、会话 ID、关键字、时间等；
20.	事件查询统计	告警检索效率高达亿条数据分钟级，搜索条件支持全范围搜索（特别要求在超过亿条数据量时），一次性完成搜索的响应时间在分钟级别；
21.		内置用户登录情况、用户访问情况、IP 访问情况、风险统计情况、统方事件报表，并支持自定义报表，支持 Word、PDF、Excel 格式导出报表；
22.		支持内置抗生素使用报表、高值耗材报表。展示医务人员用药情况、患者自费比例、抗生素使用情况、抗生素类型使用情况；展示耗材使用情况、科室使用情况；报表支持 Word、PDF、Excel

		格式导出。
23.		#支持对可疑监控对象的操作语句进行会话级的事件回放，回放时间可达前后60分钟，方便风险及违规操作的追溯；（提供截图并加盖投标人公章）
24.	审计配置管理	翻译功能：支持在审计时自动将审计结果翻译成自然语言，支持系统定义和用户自定义翻译，按照业务的行为和分类来进行信息的组织和展现，便于审计人员方便、简单的获得并了解数据库审计的结果；
25.		三权分立：提供管理员权限设置和分权管理，纪委监测用户、系统管理用户、安全规则管理用户权限分开，相应权限的用户只能查看、管理相应的功能，责任明确；
26.		支持系统管理人员异常操作监控，可按需选择需要告警的操作类别，未开启的操作类别不会发生告警。可以看到具体的告警日志信息，同时支持指定查询某时间段和某类型的告警日志查询。（提供截图并加盖投标人公章）
27.	审计数据管理	提供审计数据管理功能，能够实现对审计数据的自动备份、手动备份，支持增量、全量备份方式；
28.		提供审计数据的导出和导入功能；
29.	攻击检测能力	支持对SQL注入、跨站脚本攻击等web攻击的识别与告警；
30.		系统应具备自动发现未知仿冒进程工具的能力，通过对未知进程的监控从客户端工具使用的次数，客户端IP及次数、连接数据库次数等多维度进行安全评估和预警；（提供截图并加盖投标人公章）
31.		系统应具备防范非法IP地址、防范暴力破解登录用户密码（能够对连续失败登陆进行自动锁定，锁定时间可设置）等安全功能；
32.		系统本身应自带系统级的安全设置，对于统方和破坏数据库的危险行为如：拖库、删表、EXP备份导表等行为自动识别和告

		警；

3.2. 内网应用域防火墙（核心产品）

序号	技术指标	详细技术参数
1.	硬件要求	设备硬件≤2U,配备内存≥32G，机械硬盘≥1T，≥12 个千兆电口、≥12 个千兆光口、≥8 个万兆光口、满配对应速率千兆、万兆多模模块。≥2 个电源，≥3 个可用扩展槽位
2.	性能要求	防火墙吞吐≥60G,并发连接≥2000 万,每秒新建连接≥42 万,应用层吞吐量≥48G,FW+IPS 吞吐量≥9G,FW+AV 吞吐量≥12G,FW+WAF 吞吐量≥4.5G，全威胁吞吐量≥7G，IPSEC VPN 吞吐≥3G， SSL VPN 吞吐≥2.5G，SSL VPN 并发用户数≥5000。
3.	特征库要求	默认包含应用识别功能，包含≥1 年应用特征库升级许可；Web 应用防护特征库≥3 年升级服务许可；专业版快速扫描查杀病毒库≥3 年升级服务许可；IDP 攻击规则特征库≥3 年升级许可；
4.	工作模式	#支持路由、交换、虚拟线、Listening、混合工作模式（提供截图并加盖投标人公章）
5.	路由交换	支持 RIP、OSPF、BGP4、QinQ、PIM-SM、PIM-DM
6.		#支持策略略路由，支持根据入接口、源/目的 IP 地址、协议、用户、应用、选路算法、探测等多种条件设置策略路由（提供截图并加盖投标人公章）
7.	链路聚合	支持手动和 LACP 链路聚合，可根据源/目的 MAC、源/目的 IP、源/目的端口、五元组、端口轮询等条件提供不少于 10 种链路负载算法
8.	IP/MAC 绑定	支持 IP/MAC 绑定，支持跨三层绑定，支持 IP/MAC 绑定表导入导出，以便对 IP/MAC 绑定关系进行批量操作；

9.	地址转换	#支持多种地址转换，支持源/目的 NAT、双向 NAT、NoNAT 转换方式；支持源 IP 转换同一性；支持端口块地址转换和 EIM 地址转换（提供截图并加盖投标人公章）
10.	链路负载均衡	支持链路负载均衡功能，支持轮询、加权轮询、就近选路、优先级、带宽比率等多种链路负载均衡算法，支持备用选路算法，支持链路过载保护
11.	DNS 双向智能转换	防火墙作为 DNS 服务器可依据访问地址来源将服务器域名解析为内部地址或外部地址，同时支持通过配置多条转换策略，实现内网资源服务器的负载均衡
12.	访问控制	#支持一体化安全策略配置，可以通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、高级威胁防护、WAF、邮件安全、数据过滤、文件过滤、僵木蠕防御、审计、数据库防护、防代理、APT 等功能配置,简化用户管理（提供截图并加盖投标人公章）
13.		访问控制策略执行动作支持放行、阻断、认证、收集，对需要认证的流量进行 Web 认证，策略中可设置用户 Web 认证的门户地址或收集策略流量访问记录，生成更细粒的策略
14.		提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析、宽泛策略分析，可在 WEB 界面显示检测结果
15.	入侵防护	持独立的入侵防护规则特征库，特征总数在 5500 条以上
16.		规则库支持根据攻击类型、风险等级、流行程度、操作系统等进行分类，防护动作包括告警、阻断、记录攻击报文（提供截图并加盖投标人公章）
17.	病毒过滤	支持对 HTTP/SMTP/POP3/FTP/IMAP/IM 等协议进行病毒防御；支持 2 种专业品牌反病毒厂商病毒特征库（提供 2 家品牌防病毒厂商的合作文件证明），病毒特征库规模超过 400 万；支持对 6 级以上的压缩文件进行解压查杀；特征库数量： 专业版

		200 万+
18.	Web 攻击防护	具备预定义 Web 攻击规则库，规则总数在 1900 条以上，同时支持正则表达式或字符串方式自定义检测规则，支持对 HTTP 和 HTTPS 流量进行防护
19.		支持对 HTTP 头部的各个字段做合规性限制，可对最大请求头长度、最大 body 长度、最大请求行长度、最多 cookies 个数、最多 header 头个数等参数进行检查过滤（提供截图并加盖投标人公章）
20.	审计	支持独立审计策略，支持审计白名单

3.3. 外网核心交换机

序号	技术指标	详细技术参数
1.	链路聚合	支持静态聚合
2.		支持动态聚合
3.		支持跨设备聚合
4.	端口特性	支持 802.3x 流控（全双工）
5.		支持基于端口速率百分比的风暴抑制
6.	MAC 地址表	支持黑洞 MAC 地址
7.		支持设置端口 MAC 地址学习最大个数
8.	VLAN	支持基于端口的 VLAN
9.		支持 IP 子网的 VLAN
10.		支持协议 VLAN
11.	DHCP	支持 DHCP Client
12.		支持 DHCP Snooping
13.		支持 DHCP Relay
14.	DNS	支持静态域名解析
15.		支持动态域名解析客户端

16.		支持 IPv4 和 IPv6 地址
17.	IRF2 智能弹性架构	支持 IRF2 智能弹性架构
18.		支持分布式设备管理，分布式链路聚合，分布式弹性路由
19.		支持通过标准以太网接口等方式进行堆叠
20.		支持本地堆叠和远程堆叠
21.	IP 路由	支持 IPv4/IPv6 静态路由
22.		支持 RIPv1/v2、/RIPng

3.4. 外网业务域防火墙

序号	技术指标	详细技术参数
1.	配置要求	产品不少于 10 个 1000M 以太网电口，4 个千兆光口 SFP，2 个万兆光口 SFP+，支持 2 个 USB 口和 1 个 RJ45 串口，2U 机箱。3 层大包吞吐量≥20Gbp，网络层吞吐量≥15Gbps，应用层吞吐量≥8Gbps，并发连接数≥200 万，每秒新建连接数≥12 万。
2.	工作模式	产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。
3.	路由功能	产品支持策略路由负载，支持基于服务、ISP 地址、应用、地域等维度进行智能选路，保证关键业务流量通过优质链路转发，支持加权流量、带宽比例、线路优先等负载均衡调度算法。（提供截图并加盖投标人公章）
4.	应用识别	产品支持对不少于 9160 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。（提供截图并加盖投标人公章）
5.	地域访问控制	产品支持与国家位置信息结合设置安全策略，识别流量发起的国家或地区的位置信息，根据流量发起的国家或地区的访问位置信息实现对不同区域访问的差异化控制。

6.	双因素认证	产品支持管理员双因子认证，可以通过用户密码和 Key 等不同方式登陆产品管理界面。
7.	入侵防御	产品内置不低于 10800 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。
8.		#产品支持僵尸主机检测功能，产品预定义特征库超过 128 万种，可识别主机的异常外联行为。（提供截图并加盖投标人公章）
9.	防病毒	产品支持对多重压缩文件的病毒检测能力，支持不小于 15 层压缩文件病毒检测与处置。（提供截图并加盖投标人公章）
10.		产品支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略，需提供产品相关功能截图，并提供检测机构出具关于“勒索病毒”的相关证书证明功能有效性。（需提供相关证明并加盖投标人公章）
11.	账号安全	#产品支持用户账号安全保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。需提供产品相关功能截图，并提供检测机构出具关于“账号保护”的相关证书证明功能有效性。（需提供相关证明并加盖投标人公章）
12.	策略管理	产品支持对安全策略管理和审计功能，记录安全策略变更时间、变更账号、变更类型等内容，提升日常安全策略运维效率。
13.	产品资质	要求所投产品具备计算机信息系统安全专用产品销售许可证，提供有效证书复印件并加盖投标人公章。
14.		要求具备国家版权局颁发的软件著作权登记证书，提供相关证明材料并加盖投标人公章。
15.		要求所投产品具备 EAL4 增强级证书，提供有效证书复印件。

4. 组织实施及服务要求

4.1 投标人需根据项目的采购、建设的要求，采用成熟的软硬件产品进行投

标。产品必须满足本次项目的采购、建设的主要要求，并保证能对选用产品进行很好的集成。

4.2 投标人在中标并签署合同后，应完成采购文件中所规定的各项任务，包括：提供完善的系统建设方案、系统的安装调试、进行用户培训，并完成验收前期的各项准备工作。

4.3 投标人应向采购人提供产品或服务，承担方案中所有的集成责任。承诺与本项目的相关单位进行积极主动的合作。投标人必须服从采购人的统一协调，在系统方案设计、实施方案设计、设备供货、系统集成、技术支持、运行维护等方面相互配合。

4.4 投标人在投标文件中需提供本项目的具体组织实施方案。方案中包括但不限于以下内容：进度计划，保障措施，运输，安装，验收程序等。

（1）实施计划：根据实施周期的要求，描绘项目目标、范围，合理安排实施人员，编制进度计划，投标人应对项目实施各阶段进行合理划分，并明确各阶段应完成的工作和提交的产品及文档，采购人将对项目实施进度进行评价。

（2）项目管理：提供采购人对项目管理的理解，内容包含进度管理、质量保证、文档要求以及风险控制等内容，具体要求如下：

①在签订合同后，进行项目产品的供货，并根据采购文件中技术部分要求，配合采购人对采购的设备、软件型号、规格、数量、外型包装及资料文件（如装箱单、保修单、随箱介质等）等进行到货验收。

②提供项目所需的系统实施前调研及项目实施服务，包括硬件安装、集成、测试及调试等服务工作，做到招标文件中所有产品和原有硬件和软件系统连接正常并协同工作。

③项目实施过程中，必须同意采购人或采购人指定委托人的集成人员参与建设、检测或排除故障，并接受监督。

④投标人应严格把握项目实施质量，保证实施过程使用的工件或组件的质量。

⑤投标人应严格按照招标要求的时间进度保质保量地完成工作。

⑥按照招标文件的要求，加强项目实施过程中的文档管理。

（3）项目进度要求：60 个日历日内完成设备的上架、安装、调试等工作。

4.5 设备安装要求：投标人在货到现场后 7 个日历日之内进行设备安装，调试保证设备正常运行，同时提供计量检定证书或厂家合格证书。并指派专人负责与采购人联系售后服务事宜。

4.6 在实施工作开始和结束时，向采购人提供完整的下述资料：

（1）实施文档（包括但不限于）：实施方案、硬件设备安装与调试等过程技术文档。

（2）联合调试文档：应提供针对本项目在联通性调试过程中的文档。

（3）验收文档：

（4）产品文档（包括但不限于）：所有采购产品的安装、操作及使用手册等。

4.7 投标人在完成相关软硬件设备选型与配置和系统集成的过程中，提供相应文档，所有提交的技术文档尽可能采用中文，如正式文档为非中文则需提供英文或中文文档。

4.8 应急响应

投标人应能根据提供的产品及服务提供快速应急响应。投标人应具备完备的应急处理服务体系，应急响应服务应满足 3 分钟快速响应，60 分钟到达用户现场。

5. 售后服务要求

5.1 设备保修期内，投标人必须提供每月一次的设备巡检服务，并提供智能信息化运维管理系统用于记录巡检服务工作内容，以便采购人清晰了解巡检服务绩效；

5.2 设备保修期内，投标人必须提供每年四次的设备安全加固服务，并提供智能信息化运维管理系统用于记录安全加固工作内容，以便采购人清晰了解安全加固服务绩效；

5.3 智能信息化运维管理系统要求：提供智能信息化运维管理系统截图（不少于三张），能够清晰展示服务过程，并支持用户评价；

5.4 项目执行期间，投标人须为采购人提供项目管理软件，协助采购人记录本次项目的实施过程，项目管理软件要求如下：提供项目管理系统截图（不少于三张），能够清晰展示项目运行过程，如项目进度展示及建立项目子任务等；

5.5 投标人须为采购人提供资产管理系统以支持对本次项目所涉及资产进

行管理，以协助采购人详细记录本次项目所购买资产信息，资产管理系统要求如下：提供资产管理系统截图（不少于三张），能够记录资产详细信息，并支持维护资产属性。

5.6 硬件若任何因安装工艺、材料和产品部件、质量造成的设备或部件损坏，进行无偿更换和维修；若经修缮后仍存在质量问题，则该项保修期应予顺延。保修期内发生故障的设备如无法在 24 小时内修复，应提供备用设备以保证系统的连续稳定运行，并在 5 个日历日内修复故障设备或更换新设备，5 个日历日内不能解决的，由投标人提供替代设备保障系统正常运行，在无相同型号的同种设备时，应当更换同类设备中较高型号的产品。

5.7质保期：3年

6. 质量保障要求

投标人在项目实施过程中应严格按照相关安全标准,针对项目实施的各个环节，提出有效质量管理计划、质量控制措施及风险控制规避计划,项目经理应在项目每一阶段，对实施过程的控制，调查、分析和解决发现的问题，问题及其解决办法都应写成文档（包括项目周报、会议记录等），保证项目按目标完成。本项目质量保质期 3 年。

7. 安全保密要求

投标人要严格遵守国家《保密法》及有关保密的法律法规，选派具有良好职业道德的人员参与和从事本项目工作，服从采购人的管理，严格遵守采购人的保密规定和工作制度，并承担相应的保密责任。

投标人所有参与本项目的服务人员需签订《保密承诺书》。投标人负责对《保密承诺书》归档保管，接受采购人检查。投标人要对承诺履行情况负有监督责任，一经发现违反承诺情况，要及时向采购人报告。

投标人所有参与本项目的服务人员自觉接受采购人的安全保密监督和管理，如违反安全保密条款，采购人将追究其责任，对重大的泄密事件将移交司法部门追究其法律责任；对泄露系统资料，造成伤害的，除依据有关规定追究有关责任人员法律责任外，还应依法承担相应的民事责任。

8. 其他要求

★投标人应保证项目建设期间系统稳定运行。为保证本项目实施有序进行，

若投标人取得中标资格，应自行完成所有协调第三方软件系统开发公司协助进行系统割接与迁移的工作，以满足本项目实施需要，所产生的费用均包含在投标总价中，采购人不再为项目建设系统割接与迁移支付任何费用。

注：投标人应提供针对上述要求的加盖单位公章的承诺书原件，否则其投标将作为无效投标被否决。

9. 验收要求

验收内容和标准

1、验收内容：

1）中标人交付的货物应当完全符合本合同或者招投标文件所规定的货物、数量和规格要求。

2）中标人应将所提供货物的装箱清单、型号、外观质量、用户手册、原厂保修卡、随机资料及配件、随机工具等交付给采购人。

3）中标人应收集整理各项验收数据、文档，汇总成册，在验收时提交至采购人。

4）中标人应对设备进行冗余联通性测试。

5）中标人实施的项目符合三级等保相关规定并提供测评报告，配合完成采购人的三级等保测评工作。

2、验收标准：

中标人完成全部供货与集成服务，各硬件系统运行正常，达到采购人验收标准。

9.2 验收方式

1、项目初验：中标人完成全部供货与集成服务，各系统运行正常，并向采购人提供完整的初步验收资料、验收报告和项目初验申请，由采购人确认项目是否符合初验条件。经采购人确认符合项目初验条件后，由采购人在 10 个日历日内启动项目初验程序。

2、试运行：项目初验合格之日起，系统进入为期 1 个月的试运行期。试运行期内，中标人须做好故障的处理工作及运维保障。

3、项目终验：试运行期满后，中标人完成合同全部义务且系统运行稳定，中标人应向采购人提供完整的项目终验材料及终验申请。由采购人在收到中标人

项目终验申请后确认项目是否符合项目终验条件。经采购人确认符合项目终验条件后，由采购人在10个日历日内启动项目终验程序。

4.采购人须在上述各阶段验收后5个日历日内给予批准或提出整改意见。投标人须按要求修改，并承担由自身原因造成整改的费用。

5.采购人对项目的终验合格，不能排除投标人的产品质量责任和工程质量责任，投标人需按合同约定继续履行责任。