杞县妇幼保健院医疗设备采购项目（第一批）

五包：网络安全加固建设设备采购

项目合同书

甲方：杞县妇幼保健院

乙方： 河南慧家乐智能设备有限公司

签订日期:

本合同由以下双方在【杞县】签订：

甲　　方	杞县妇幼保健院		
通讯地址	开封市杞县金城大道中段		
电　　话	0371-22059277	传　　真	
法定代表人	倪倩		
开户银行			
帐　　号			
纳税号	124102214164455806		
注册地址			
联系人	姓名：　王龙	电话：0371-22059277	

乙　　方	河南慧家乐智能设备有限公司		
电　　话	0371-63659801	传　　真	0371-63659801
法定代表人	孟伟杰		
开户银行	中国工商银行股份有限公司郑州科学大道支行		
帐　　号	1702 1213 0920 0091 708		
统一社会信用代码	91410100096264245Y		
注册地址	郑州高新区长椿路 11 号 13 幢 1 单元 16 层 159 号		
商务联系人	姓名：姚建光	手机：16637155810	
技术联系人	姓名：黄亚萍	手机：13023827156	

根据《中华人民共和国政府采购法》、《中华人民共和国合同法》等法律法规的规定，甲乙双方按照招标结果（项目名称：杞县妇幼保健院医疗设备采购项目（第一批）、五包：网络安全加固建设设备采购，项目编号：汴杞财招标采购-2021-115-5）签订本合同。

一、合同标的

产品名称	参数要求		数量	品牌型号	单价（元）	总价（元）
数据库审计	规格性能	标准1U机架式专用安全设备，交流单电源，2个USB接口，1个RJ45串口，1个GE管理口，≥6个GE电口，≥1个接口扩展槽位，≥2T SATA硬盘，含数据库审计模块，吞吐量＞100Mbit/秒。	1台	绿盟、DASNX3-HDB590	43562	43562
	自动发现	支持数据库自动发现，设备无需添加、即插即用				
	支持的数据库类型	支持主流数据库：Oracle、SQL Server、MySQL、DB2、Sybase、PostgreSQL、Informix、DM、Oscar、Kingbase、Gbase、Hbase、MongoDB、HIVE、Redis、Cache。				
	协议支持	支持在IPV6环境中部署，且支持所有数据库IPV6协议的审计。				
	部署方式	旁路镜像：旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计				
		★Agent方式：支持在目标数据库安装Agent解决无法通过旁路镜像获取流量的场景，如同服务器部署数据库和应用系统、云环境、虚拟化环境场景下数据库的审计。要求提供功能截图证明				
		分布式部署：支持分布式部署，审计引擎和审计中心都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展。管理中心可实现统一配置、统一报表生成、统一查询。				
	审计内容	支持审计到前端的应用用户、数据库用户名、主机名称、操作系统用户等；				
		执行结果ResultSet：执行成功与否的结果以及返回结果集，如查询操作的返回内容；				
		准确审计长SQL语句；有效分割、准确审计多SQL语句；准确审计绑定变量的SQL语句				
	加密链路审计	支持MySQL数据库的SSL/TSL加密链路审计				
	数据库安全监测	能对基于数据库漏洞进行攻击行为监测和告警，支持200个以上的数据库漏洞攻击规则库				
		通过模式匹配的方式对SQL访问进行监测与告警，判断是否为可疑SQL注入；提供SQL注入特征库				
	告警策略	支持敏感语句告警策略。支持自定义添加敏感语句和信任语句；				
		支持根据风险操作、SQL注入、漏洞攻击检测、语				

		句管理等模块定义告警规则，支持高、中、低风险告警，支持系统资源监控与告警。				
	响应方式	根据不同的安全级别采用不同的响应方式，包括记录、告警；告警方式包括：邮件、短信、SYSLOG、SNMP				
	IP 别名	支持客户单 IP 建立别名，所有涉及客户端 ip 页面均显示业务化 ip 名称。				
	审计查询	支持基于时间、IP 地址、数据库服务器 IP 地址、用户名、数据库操作命令、数据库表名，执行结果，应用用户等多种丰富的查询检索条件。				
	敏感信息遮蔽	★对审计结果集敏感内容可进行屏蔽，要求提供功能截图证明				
	旁路阻断	★对于高风险操作所在的会话，支持旁路阻断功能，避免更大的危害，要求提供功能截图证明				
	报表展示	支持报表自定义，自定义项不少于 10 种。				
	系统自身安全性	根据三权分立的原则。提供系统管理员、安全管理员和审计管理员不同的用户身份验证。				
	产品资质	产品具有中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品认证证书》（增强级），提供有效证书的厂商盖章复印件				
		产品具有《信息技术产品安全测评证书》（EAL3+）（千兆），提供有效证书的厂商盖章复印件。				
		产品具有 IPv6 Ready 认证证书，提供有效证书的厂商盖章复印件。				
	厂商资质	厂商获得由中国信息安全测评中心颁发的信息安全服务(安全开发类二级)资质证书，提供有效证书的厂商盖章复印件				
		厂商为 2021 年-2023 年河南省网信系统网络安全工作支撑单位，提供证明材料，加盖厂商公章				
		厂商获得由中国信息安全测评中心颁发的信息安全服务(安全工程类三级)资质证书，提供有效证书的厂商盖章复印件				
	其它	提供三年质保服务				
终端安全系统	规格性能	含终端安全管理平台 1 个，windows 客户端授权 150 个点。windows 服务器授权 6 个点。	1 套	金山终端安全系统、KSV9	47595	47595
		提供病毒防护、漏洞管理 、边界管理、软件管理、IP/MAC 管控、网络管控、XP 防护盾、流量管控等功能。				
	控制中心操作系统支持	Windows Server 2008（64 位）/Windows Server 2012 （64 位）、中标麒麟/银河麒麟/Deepin/SUSE Linux/Red Hat Linux/centOS/Ubuntu 12 以上版本				

	客户端操作系统支持	Windows XP_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10/ Windows Server 2003_SP2/Windows Server 2008/Windows Server 2012/Windows Server 2016/中标麒麟/银河麒麟/Deepin/中科方德/SUSE Linux/Red Hat Linux/centOS/Ubuntu 12以上版本				
	系统部署管理	控制中心：采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能。				
		客户端：与系统控制中心通信，提供控制中心管理所需的相关数据信息；执行最终的木马病毒查杀、漏洞修复等安全操作。				
		支持多种分组规则，如IP分组以及支持与AD、LDAP同步功能，可将用户组织架构同步到终端安全管理系统中，依照用户现有架构进行管理。分组支持无限层次分组，支持生成组安装包，安装后自动进入该分组。（提供功能截图，并加盖公司公章）				
	即时通讯防护	支持检测QQ、MSN、阿里旺旺等常用聊天软件传输文件的安全性，确保传输文件不中毒；				
	移动设备病毒防护	要求提供U盘等移动设备接入电脑自动检测功能，全面拦截和清除在移动设备接入系统可能带来的病毒木马；				
	浏览器防护	支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置（提供功能截图，并加盖公司公章）				
	边界文件追溯功能	可根据设定好的固定区域对未知威胁文件及黑文件进行定向追溯，实现对所有可疑威胁文件进行全周期追踪				
	虚拟补丁	支持虚拟补丁功能，拦截外部黑客工具通过利用弱口令集和密码表，对目标机器的网络共享发起高频率的操作请求，以达到攻破目标机器的密码并在目标机器上释放运行病毒文件的行为。				
	压缩包杀毒	支持文件解压缩病毒查杀，支持对zip、rar、7z等多种格式的压缩文件查杀能力；默认支持32层压缩扫描，且用户可以自定义设置扫描层数				
	病毒查杀	有针对宏病毒的专杀模块，可以提供针对宏病毒的专属解决方案；				
		★须提供原厂商关于检测和清除可移植可执行文件中感染型病毒方法的证明文件复印件。				
	边界文件追溯功能	可根据设定好的固定区域对未知威胁文件及黑文件进行定向追溯，实现对所有可疑威胁文件进行全周期追踪				

	敲诈者病毒防御	★对勒索者病毒提供防护机制，采用虚拟钓饵方式有效拦截勒索者病毒（提供功能截图，并加盖公司公章）				
	病毒库升级	要求支持服务器端病毒库的定时更新和手动更新两种升级模式。				
	补丁分发与漏洞修复	支持自定义补丁排除名单，防止终端打补丁后造成系统或业务进程崩溃；				
		终端支持智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁（要求提供截图）；				
	资产管理	支持统计指定分组或全网的终端扫描数、终端管理软件安装数、未安装终端数及安装率				
	日志报表	要求支持邮件报警，可以设定多种触发条件，满足条件后自动发送邮件到相关人。邮件触发条件至少包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等				
		提供大数据分析系统，可将全网发现的威胁文件通过 MD5 值按照黑名单、白名单、灰名单进行添加分类，有效防止未知威胁攻击				
	流量管理	可统计指定终端网络的上传，下载速度与流量；				
	主机防火墙	具备主机防火墙功能，可置主机防火墙(网络管控)策略，能有效防护全网终端免受网络安全攻击。支持对 IP、端口协议及访问方向等维度过滤，能智能识别网络协议，严格的端口管理减少端口暴露而带来的病毒传播、安全攻击等机率				
	管控环境	终端支持在线、离线两种策略，可同时使用在线或离线两种状态，保证终端安全运行。				
	XP 防护	支持 Windows XP 系统补丁修复功能				
	其他	提供三年质保服务和三年病毒库升级服务。				
日志审计系统	规格及性能	标准 1U 机架式专用安全设备，交流冗余双电源，专用硬件平台和安全操作系统；≥4 个千兆 SFP 插槽，≥6 个千兆电口，2 个 USB 接口，1 个 RJ45 串口，1 个 GE 管理口，≥1 个接口扩展槽位（支持万兆扩展），支持多端口采集，存储容量≥4TB，本次提供不少于 100 个日志源授权许可，日志处理性能≥3000EPS	1 台	绿盟、LASNX3-HD1000	95383	95383
	监测范围	管理范围包括但不限于网络安全设备、网络设备、数据库、中间件、操作系统、应用系统等。				
	系统部署	系统应支持 IPv4、IPv6 环境下部署				
		系统应支持 NAT 场景的日志采集				
	数据采集	系统内置采集器，不依赖其他设备即可进行日志采集；				

		系统支持配置外置采集器，外置采集器数据应提供加密压缩传输，以确保数据安全以及传输效率。				
		系统支持的数据采集方式包括但不限于 SYSLOG、RSYSLOG、SNMP Trap、FTP、ODBC、JDBC、Netflow、WMI、二进制数据、专用 Agent 等方式采集日志				
	日志管理	系统应能实现海量日志数据的采集并保存原始日志数据；系统应能够对异构日志格式进行统一化处理并保存统一化处理后的日志数据				
		系统应支持范式化日志多级提取，支持正则、KV、格式串等多种灵活的提取方式				
		系统应支持 IPv4、IPv6 日志数据的采集、范式化、分析、展示				
		★系统应支持日志源监控能力，包括采集器维度及资产维度的监控，资产维度支持展示资产详细信息，要求提供功能截图证明				
	日志转发	系统应提供日志转发功能，应支持日志转发多个目标地址，可实现原始日志、范式化日志的转发，且不丢失原始日志源 IP 信息				
	日志检索	支持支持索引检索；hive 查询；支持常见类型的条件查询语法，查询语法统一处理；				
		支持日志分组管理功能，可将查询条件分类固化，便于常规性统计分析。				
		支持可根据新接入的日志，自动更新日志检索中的日志类型和各类日志属性字段，新接入日志天然支持检索功能，无需单独开发。				
	日志存储扩展	★系统应支持以 NFS 网络共享存储扩展的方式进行日志存储扩展，要求提供功能截图证明				
	资产管理	★系统应支持资产属性配置，且支持资产标签，且至少 6 种标签以上，根据标签可快速查询资产，要求提供功能截图证明				
		系统应支持手工注册资产，支持对资产进行修改/删除、批量导入/导出/添加/修改/删除等多种方式的管理；				
		系统应支持从日志进行资产发现；				
		★系统应支持资产以拓扑图形式展示，鼠标移动至资产图标可展示对应的资产信息，要求提供功能截图证明				
	安全事件管理	系统应内置事件分类，并支持自定义事件分类，可定义事件分类的风险级别；				
		系统应内置丰富的事件规则，应支持自定义事件规则。				
		系统支持查询实时事件，并可以很方便的下钻事件规则以及原始日志信息。				
	统计与报	系统应能支持自定义报表目录、LOGO 等				

	表					
	产品资质	产品具有《中国国家信息安全产品认证证书》（增强级），提供有效证书的厂商盖章复印件				
		产品具有《信息技术产品安全测评证书》(EAL3+)，提供有效证书的厂商盖章复印件。				
		产品具有 IPv6 Ready 认证证书，提供有效证书的厂商盖章复印件				
	厂商资质	厂商获得由中国信息安全测评中心颁发的信息安全服务(安全开发类二级)资质证书，提供有效证书的厂商盖章复印件				
		厂商获得由中国信息安全测评中心颁发的信息安全服务(安全工程类三级)资质证书，提供有效证书的厂商盖章复印件				
		厂商为 2021 年-2023 年河南省网信系统网络安全工作支撑单位，提供证明材料，加盖厂商公章				
		厂商为微软 MAPP 计划合作伙伴，提供证明材料，加盖厂商公章。				
	其他	提供三年质保服务				
上网行为管理	规格性能	标准 1U 机架式专用安全设备，≥10 个千兆电口，≥4 个千兆 Combo 接口（光电复用），≥500G 硬盘。含上网行为管理、流量管理、IPSec VPN 等功能。	1台	绿盟、SASNX3-WB3320	30060	30060
	产品架构	多核架构设计，不允许采用 X86 架构，功能采用模块化结构设计。				
	重置插孔	★支持外置 Reset 重置插孔，一键恢复出厂设置，并提供设备外观照片证明				
	部署模式	支持路由模式、透明（网桥）模式、旁路模式、混合模式，支持将多个物理网口加入一个网桥中；部署模式切换无需重启设备；支持镜像和被镜像；				
	路由支持	支持静态路由、策略路由、动态路由、ISP 路由；策略路由支持七元组策略；动态路由支持 RIP、OSPF 等；ISP 路由支持运营商地址自定义；				
	IPv6	支持配置基于用户和应用均为任意的 7 元组的 IPv6 策略，支持 IPv6 数据包安全检测机制，可有效防御异常包攻击				
	4G 支持	★支持 4G 扩展网卡，支持在 4G 接口上运行 IPSec VPN ，要求提供配置界面截图证明				
	链路负载	支持 7 元组的链路负载均衡策略,支持基于域名的负载均衡策略				
	服务器负载	支持 5 元组的负载均衡策略；负载算法支持权重、源地址散列+权重；支持服务器健康检查和会话保持				
	DNS 透明代理	支持基于优先级、权重的 DNS 代理算法，支持静态域名配置，支持特定域名特定 DNS 服务器解析，				

		静态域名和特定域名支持模糊匹配				
	用户行为审计	支持即时通讯应用管控的精细化管理；				
		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；				
	应用协议识别	支持主流P2P、IM、在线视频、网络游戏、网络炒股等应用识别，可识别应用数大于3500种； 支持自定义应用，可基于协议、端口、IP、域名等维度定义未知应用；支持指定应用组				
	流量管理	支持通道化的QoS策略，支持基于源地址、用户、服务、应用、时间等条件，配置保障带宽、限制带宽、带宽借用、每IP带宽、每用户带宽、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				
	入侵防御	支持软件bypass（CPU and 内存高于70%），阀值可自定义设置				
		支持针对Web服务器防护，包括网页防爬虫、脆弱口令、CGI攻击、Web漏洞等				
		系统定义超过4000+条主流攻击规则，包含Backdoor、bufferoverflow、dosddos、im、p2p、vulnerability、scan、webcgi、worm、game。				
	会话管理	★支持进行IP、整机会话限制和新建会话限制，要求提供配置界面截图证明；				
		★支持基于源IP，目的IP会话数排名，支持展示实时会话情况，包括源地址、目的地址、端口、协议，存活时间等信息，要求提供配置界面截图证明				
	用户认证功能	支持portal、微信、短信等认证方式；				
		支持用户标签，可根据用户访问信息生成访问类型标签，并将用户标签同步至Portal服务器，Portal服务器向用户推送预定义页面				
	VPN	支持IPSecVPN、SSLVPN接入，内置VPN硬件协处理器,实际配置支持DES、3DES、AES加密算法				
	端口镜像	支持端口镜像功能，支持入流量、出流量和双向流量等维度镜像				
	产品资质	产品具有《信息技术产品安全测评证书》(EAL3+)，提供有效证书的厂商盖章复印件。				
		产品具有IPv6 Ready认证证书，提供有效证书的厂商盖章复印件。				
	厂商资质	厂商获得由中国信息安全测评中心颁发的信息安全服务(安全开发类二级)资质证书，提供有效证				

		书的厂商盖章复印件				
		厂商为微软 MAPP 计划合作伙伴，提供证明材料，加盖厂商公章。				
		厂商为 2021 年-2023 年河南省网信系统网络安全工作支撑单位，提供证明材料，加盖厂商公章				
		厂商获得由中国信息安全测评中心颁发的信息安全服务(安全工程类三级)资质证书，提供有效证书的厂商盖章复印件				
	其他	提供三年质保服务及三年上网行为特征库升级服务				
下一代防火墙	规格性能	标准 1U 机架式专用安全设备，≥4 个 GE 电口，1 个 RJ45 串口，1 个 RJ45 管理口，2 个 USB 接口，≥1 个接口扩展槽位，网络层吞吐≥3G；含防火墙、流量管理、应用管理、IPSec VPN 等功能。	1 台	绿盟、NFNX3-HDB1211-1	26200	26200
	防火墙功能	支持虚拟线、二层透明、三层、混合、旁路监听接入方式，适应各种网络环境需求				
		提供基于源/目的 IP 地址、安全区、应用/应用过滤器、协议/端口、时间、用户、安全模板/模板组的精细粒度的安全访问控制				
		支持基于策略的双向 NAT、动态/静态 NAT、端口 PAT				
		支持 OSPF、RIP、BGP、策略路由、Vlan 路由、单臂路由、反向路由、ISP 路由、DHCP 、DNS、Vlan Trunk				
		支持链路探测，能够在每接口上以 ICMP/TCP/UDP 协议探测目标主机可达性，探测链路是否有效				
		支持汇聚接口，支持手动绑定汇聚接口				
		支持 IPSEC VPN、SSL VPN、L2TP VPN；支持账号本地认证/Radius 认证/LDAP 认证等				
	流量控制	★支持用户以安全区、IP 地址（网段）、时间、用户、应用多维度的对流量进行管理和控制，包括限制应用上下行最大带宽、保证应用上下行最小带宽、保证带宽下的优先级排序以及每 IP 的进行应用流量控制，能够提供《一种网络数据传输速率控制设备及方法》的技术证明，要求提供证明文件复印件。				
	资产识别	支持不安装任何客户及插件的方式且不通过主机扫描等技术，识别内网主机的操作系统、杀毒软件、浏览器等信息。				
		★可自定义操作系统、浏览器、杀毒软件的风险等级，并支持预置风险等级，要求提供配置界面截图证明。				

		可为每个内网主机生成风险指数，通过数字直观展示内网主机的风险状态，资产风险涵盖了操作系统、浏览器、杀毒软件、应用、流量、服务等内容。				
	应用识别	★支持应用过滤器，至少支持 4 个维度进行过滤，比如：应用类别、实现技术、风险等级、标签，要求提供配置界面截图证明				
		能够将通过应用过滤器筛选出来的应用直接生成模板供用户统一管理使用。				
	无线管控	支持识别内网中无线热点，并对热点进行允许或阻断控制				
	漏洞虚拟补丁	★支持联动外部扫描器，外部扫描器定期将漏洞推送至防火墙，通过防火墙可查看扫描器上报的内部资产漏洞的拦截情况,要求提供配置界面截图证明				
	产品资质	产品具有《自主原创产品测评证书》，提供有效证书的厂商盖章复印件				
		产品具有《国家信息安全漏洞库兼容性资质证书》，提供有效证书的厂商盖章复印件				
		产品具有《信息技术产品安全测评证书》(EAL4+)，提供有效证书的厂商盖章复印件				
	厂商资质	厂商获得由中国信息安全测评中心颁发的信息安全服务(安全开发类二级)资质证书，提供有效证书的厂商盖章复印件				
		厂商获得中国信息安全测评中心颁发的信息安全服务(安全工程类三级)资质证书，提供有效证书的厂商盖章复印件				
		厂商为微软 MAPP 计划合作伙伴，提供证明材料，加盖厂商公章。				
		厂商为 2021 年-2023 年河南省网信系统网络安全工作支撑单位，提供证明材料，加盖厂商公章				
	其他	提供三年质保服务。				
安全隔离与信息交换系统	系统架构	采用 2+1 系统架构即内网单元+外网单元+FPGA 专用隔离硬件，不能采用网线等形式直通。	1台	绿盟、SIESNX3-HDB1010	40800	40800
		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。				
	规格性能	标准 1U 机架式网闸，采用双主机架构，内网≥4 个千兆电口，1 个 RJ45 串口和 2 个 USB2.0 口；外网≥4 个千兆电口，1 个 RJ45 串口和 2 个 USB2.0 口；交流单电源。吞吐量≥300Mbps				
	内置模块	系统内置安全浏览、邮件发送、文件同步、实时数据库、关系数据库、MODBUS、组播代理、用户自定义等应用模块,并可控制协议的的动作、参数、内容。				

	MODBUS 模块	支持 MODBUS 协议传输代理模块，可按照用户需求控制具体功能代码及值域等参数，比如只允许读取，不能设置，只允许设置某一线圈的值在某个范围等；				
	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				
	视频应用	兼容主流视频传输及控制协议。				
		支持 GB28181 视频通信国家标准。				
		★支持 SIP 信令控制，可控制云台，要求提供功能截图证明。				
		★支持海康、大华、华为、华三、公安一所、天地伟业、天视达、宇视、科达、数码视讯、藏愚、合众、汉邦等视频厂商，要求提供功能截图证明。				
	数据同步	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；				
		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。				
	组播支持	★系统支持组播代理功能，组播类型支持 ASM、SSM、SFM 多种类型，要求提供功能截图证明。				
	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关内网可信端管理接口进行配置。				
	管理用户	采取系统策略配置管理员、安全管理员与日志管理员三种角色分立的权限分配模式，用户只能维护操作本类基础管理角色的功能与操作，权限各不交叉。				
	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				
	时间模式	★支持根据时间自动切换的安全策略。支持时间段以 24 小时制，支持以星期为周期，支持指定时				

		间点一次性运行，要求提供功能截图证明。				
	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	系统支持加密的 WEB 方式管理。				
	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。				
	产品资质	产品具有《计算机信息系统安全专用产品销售许可证》（增强级），提供有效证书的厂商盖章复印件				
		产品具有 IPv6 Ready 认证证书，提供有效证书的厂商盖章复印件。				
	厂商资质	厂商获得由中国信息安全测评中心颁发的信息安全服务(安全开发类二级)资质证书，提供有效证书的厂商盖章复印件				
		厂商为 2021 年-2023 年河南省网信系统网络安全工作支撑单位，提供证明材料，加盖厂商公章				
		厂商获得中国信息安全测评中心颁发的信息安全服务(安全工程类三级)资质证书，提供有效证书的厂商盖章复印件				
	其他	提供三年质保服务。				
下一代防火墙	规格性能	标准 1U 机架式专用安全设备，1 个串口，1 个管理口，2 个 USB 接口，2 个 GE 电口，≥2 个万兆光口，≥8 个 como 接口，网络层吞吐≥5G，提供≥100SSL VPN 用户，含防火墙、流量管理、应用管理、IPSec VPN 等功能。	1 台	绿盟、NFNX3-HDB1600	26400	26400
	策略管控	能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP 地址、端口、域名组、URL 分类、接入类型、终端类型、设备组、内容安全统一界面进行安全策略配置；				
	IPV6	支持 IPv6 over IPv4 GRE 隧道，6RD 隧道；				
	协议识别	★支持识别国标 SIP 协议及主流安防厂家的私有协议；（提供功能截图）				
	流量控制	可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等；				
		支持基于用户，IP 的带宽保证；				
		★支持用户流量配额管理；（提供功能截图）				
		支持流量整形；				
	策略管理	支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维；				

		支持将基于端口的安全策略转换为基于应用的安全策略，分析设备策略风险，及冗余策略，提供安全策略优化建议				
	数据安全	★支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证、信用卡、银行卡、社会安全卡号等类型进行匹配；（提供功能截图）				
		支持 DNS 过滤，提高 WEB 网页过滤的性能；				
	DDoS 防护	支持 HTTP、HTTPS、DNS、SIP 等应用层 Flood 攻击，支持流量自学习功能，可设置自学习时间，并自动生成 DDoS 防范策略				
	NAT	支持全面 NAT 功能，对多种应用层协议支持 ALG 功能，包括 ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS 等；				
		支持源 NAT 自动探测并排除 NAT-IP 地址池中无效地址（防封杀）；				
		支持源 NAT 地址池使用率超限告警；				
		支持三元组 NAT smart-fullcone；				
		支持基于场景进行策略入侵防御的模板定制；				
		支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；				
		支持恶意域名过滤，实现对 C&C 进行阻断；				
		可以支持 HTTP、FTP、SMTP、POP3、IMAP、NFS 等协议的病毒防护；				
	上网用户认证	★支持 AD 单点登录，Radius 单点登录，NTLM 认证，免认证，与认证服务器配合实现微信认证，MAC 认证；（提供功能截图）				
	可靠性	支持 HA 平滑升级，升级窗口中支持不同版本的软件形成双机热备；				
	多出口智能选路	可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式；				
	产品资质	产品具有《自主原创产品测评证书》，提供有效证书的厂商盖章复印件				
		产品具有《国家信息安全漏洞库兼容性资质证书》，提供有效证书的厂商盖章复印件				
		产品具有《信息技术产品安全测评证书》（EAL4+），提供有效证书的厂商盖章复印件				
	厂商资质	厂商获得由中国信息安全测评中心颁发的信息安全服务（安全开发类二级）资质证书，提供有效证书的厂商盖章复印件				
		厂商为微软 MAPP 计划合作伙伴，提供证明材料，加盖厂商公章。				
		厂商获得中国信息安全测评中心颁发的信息安全服务（安全工程类三级）资质证书，提供有效证书				

		的厂商盖章复印件				
		厂商为2021年-2023年河南省网信系统网络安全工作支撑单位，提供证明材料，加盖厂商公章				
	其他	提供三年质保服务。				
等保测评	1.A信息系统定级备案（变更）服务：梳理医院HIS、LIS、PCS和EMR系统基本情况，协助客户单位完成信息系统等保备案工作，取得公安机关颁发的备案证明。 2.信息系统安全等级保护测评：针对医院HIS、LIS、PACS和EMR系统实施等级保护测评活动。 依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019），通过静态评估、现场测试、综合评估等相关环节和阶段，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、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、安全运维管。	4个	国产、HIS、LIS、PACS和EMR	22500	90000

二、结算方式及付款期限

2.1甲乙双方之间发生的一切费用均以人民币进行结算及支付。

2.2合同总额：人民币：400000元，大写：肆拾万元整。

2.3本合同签订后【 15 】天内，甲方支付货款人民币：160000元，大写：壹拾陆万元整。付款方式以汇款方式支付。

2.4乙方协助开封市杞县妇幼保健院完成等级保护备案工作后20天内，甲方向乙方支付款项人民币：120000元，大写：壹拾贰万元整，完成条件以公安机关向等保测评公司出具网络安全等级保护备案证明，并向开封市杞县妇幼保健院交付本次测评报告时间为准。

2.5乙方协助开封市杞县妇幼保健院完成等级保护备案证明，并完设备调试正常运营后3个月内甲方支付货款人民币：120000元，大写：壹拾贰万元整。

2.6乙方为甲方开具等额增值税发票。（材料为13%的税率，技术服务为6%的税率）

三、质量担保与售后服务

3.1提供自产品到货之日起，【 3 】年内免费的原厂技术服务支持。

3.2到货之日起三个工作日内，甲方验收产品，逾期则视为甲方已验收。

3.3第三方生产的产品应符合该厂商的企业标准

四、双方职责

4.1甲方责任与义务：

（1）甲方须按本合同规定按期向乙方支付首批订货款和到期款项。

（2）产品到达指定地点后，甲方应立即组织人员在当日内验货。如有异议，甲方应在乙

方交货后48小时内提出书面说明，否则视为验货合格。

（3）合同所订购之产品运抵甲方所在地后，视为交货完成。因保管不善所造成的损失，由甲方承担。

（4）如无质量问题，所有产品不允许退货。否则视为买方违约。

4.2乙方责任和义务：

（1）乙方应在合同规定时间内交货。

（2）乙方应提供给甲方的设备为符合原厂出厂标准的商品，完全符合本合同规定的质量、规格和性能。

（3）甲乙双方开箱查验时，若发现产品与清单不符，由乙方负责与原厂商协商，进行调换或补足。

五、产品所有权的转移及保留

5.1甲方未将本合同价款全部支付给乙方之前，乙方享有对产品的全部所有权；

5.2甲方在将本合同价款全部支付给乙方之后，取得产品的所有权，但该批产品中由乙方自主开发的软硬件等技术的知识产权仍属于乙方。

六、产品风险转移

6.1乙方将产品交付给甲方后，产品毁损、灭失的风险由甲方承担；

6.2甲方应履行接受产品的义务。甲方违反约定没有在约定的交付时间接受产品，或因甲方原因致使产品不能按照约定期限交付的，甲方应自违反约定之日起承担毁损、灭失的风险。

七、违约责任

7.1本合同生效后，双方应本着诚实信用原则，不得违反。如任何一方违反本合同约定，或单方面解除合同，均要向对方赔偿由此带来的全部损失。若有定金，如果乙方单方面解除合同，应立即返还甲方所付定金。若甲方解除合同，则甲方无权要求返还定金。

7.2甲方必须按本合同规定按期向乙方支付提货款和到期款项。如甲方逾期支付，则每逾期一日（工作日），乙方须按合同总金额的1‰收取甲方违约金，但金额总数不超过合同额的5%。

八、不可抗力

8.1甲、乙双方的任何一方由于不可抗力的原因（如战争、自然灾害或厂商生产等的影响）不能履行合同时，应尽快以电报、传真方式通知对方不能履行或不可以完全履行的理由，经双方确认后，作为以后检查和确认的依据。

8.2因不可抗力的原因而被迫停止或推迟合同的执行时，则合同执行相应顺延，顺延的时间等于不可抗力发生作用的时间。受影响一方应在不可抗力终止或排除后尽快传真通知对方。

在不可抗拒因素影响合同执行超过九十天的情况下，双方应达成继续执行合同的协议或双方另行协商延长本合同履行或加订合同。

九、保密协定

9.1甲乙双方均需要对此次采购商品价格进行保密，不得向第三方泄露，否则所引起之后果，损失方可向泄露方追偿损失及要求承担相应法律后果。

十、仲裁与诉讼

10.1双方对执行合同发生的争执，本着双方友好协商的原则解决。

10.2经协商不能解决的，可按照《中华人民共和国合同法》之规定提交郑州市人民法院诉讼。

十一、合同效力

11.1合同由双方单位授权代表签订。本合同自双方签字盖章之日起生效。传真有效。

11.2合同执行期内，甲、乙双方均不得随意变更或解除合同。合同如有未尽事宜，须经双方共同协商，做出补充规定，补充规定及其合同附件具有同等效力。

11.3本合同未尽事宜，双方另行订立补充协议。补充协议与本合同有冲突时，以补充协议为准。补充协议自双方签字盖章之日起生效，其有效期限与本合同相同。传真有效。

11.4甲、乙双方如需修改本合同数量、单价、金额、内容及改变交货期限或增加产品，应在合同生效后五个工作日内提出，经双方协商书面确认后生效，再另立合同。本合同正本一式肆份，双方各执贰份。

甲、乙双方的授权代表在下面签字并盖章，表示同意本合同的所有条款及条件。

甲　方：杞县妇幼保健院

代表人签章：

日期：

乙　方：河南慧家乐智能设备有限公司

代表人签章：姚建忙

日期：2021年12月21日