府谷县中医医院网络安全建设服务及设备采购项目

第一、采购需求：

1、项目名称：府谷县中医医院网络安全建设服务及设备采购项目

2、预算金额：984908.00 元

3、采购需求：外网防火墙、入侵防御系统、全网行为管理、服务器防火墙、日志审查系统、堡垒机、数据库审查、web 应用防护系统、漏洞扫描系统、网闸、态势感知、零信任网管等 13 部分。

资金来源：财政资金

一、商务要求

1）项目地点：府谷县中医医院

2）供货期（工期）：合同签订之日起 30 日历天

3）质保期：验收合格后 1 年

4）款项结算

由采购人负责结算，付款前，供应商必须向给采购人开具全额发票。付款方式：设备安装、调试、培训、验收合格后付合同款 95%，剩余 5%一年后一次付清。

5）违约责任

按《民典法》中的相关条款执行。未按合同或招标文件要求提供服务或服务质量不能满足采购人要求的，采购单位有权单方终止合同，甚至对供应商违约行为进行追究。

6）后期服务：在质保期内，如发生任何质量问题，对用户的维护要求保证在 24 小时内做出响应。接到用户要求后，售后服务人员 48 小时内到达现场，但存在不可抗力因素（自然及环境因素）除外。

二、技术要求

序号	产品名称	功能参数	数量	单位
1	互联网边界防火墙	1.网络层吞吐量≥10G，应用层吞吐量≥5G，防病毒吞吐量≥1G，IPS 吞吐量≥800M，全威胁吞吐量≥600M，并发连接数≥200 万，HTTP 新建连接数≥6 万，IPSec VPN 最大接入数≥800，IPSec VPN 吞吐量≥500M，标准 1U 设备，内存≥8G，硬盘容量≥128G SSD，单电源，接口：≥8 千兆电口+2 万兆光口 SFP+。 2.产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求，支持旁路模式。 3.支持独立的入侵防护规则特征库，规则库支持根据漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等进行分类，特征总数在 10000 条以上，能对常见漏洞进行安全防护。 4.支持独立的 WAF 防护模块，WAF 防护特征总数在 4500 条以上，支持针对地址、应用设置 WAF 白名单，支持攻击规则搜索以及自定义。 5.支持服务器抗恶意扫描功能，产品针对扫描源 IP 进行日志记录，并对恶意源 IP 联动封锁。 6.支持基于信誉的僵尸网络防护能力，具备可以持续升级的信誉库，当前僵尸网络信誉库超过 120 万种。 7.★支持 IPSecVPN 链路优化功能，在高丢包场景下，依然保障业务流畅访问体验。（需提供证明材料并加盖厂商公章） 8.支持多对一、一对多和一对一等多种地址转换方式。 9.★支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口，提高链路带宽和链路可靠性。（需提供证明材料并加盖厂商公章） 10.★所投产品厂商应具有国家信息安全漏洞库（CNNVD）技术支撑单位等级证书(一级)。（需提供证明材料并加盖厂商公章） 11.★所投产品的生产厂商需参与制定《信息安全技术 第二代防火墙安全技术 要求》。（需提供证明材料并加盖厂商公章） 12.提供三年产品质保和软件升级服务。	2	台

2	入侵防御系统	1.网络层吞吐量≥4G，应用层吞吐量≥2G，防病毒吞吐量≥600M，IPS 吞吐量≥600M，全威胁吞吐量≥450M，并发连接数≥200 万，HTTP 新建连接数≥6 万，IPSec VPN 最大接入数≥300，IPSec VPN 吞吐量≥270M，标准 1U 设备，内存≥4G，硬盘容量≥128G SSD，单电源，接口：≥8 千兆电口+2 千兆光口 SFP。 2.支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能。 3.访问控制规则支持基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组的细化控制方式，支持长连接功能并可以配置连接时长。 4.★支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、地域、认证用户、子接口和 VLAN 等因素实现对象的流量控制。（需提供证明材料并加盖厂商公章） 5.支持针对 SMTP、POP3、IMAP 邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件异常账号检测等，支持根据邮件附件类型进行文件过滤；支持针对 HTTP、FTP 协议内容检测与病毒查杀。 6.★支持同访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间。（需提供证明材料并加盖厂商公章） 7.支持恶意域名重定向功能，用于 DNS 代理服务器场景下定位内网感染僵尸网络病毒的真实主机 IP 地址。 8.支持基于攻击阶段图的方式来匹配并展示当前用户遭受到攻击的具体所处状态，并详细给出针对性处理建议，便于用户快速响应安全问题。 9.★所投产品的生产厂商具有 CCRC 颁发的信息系统安全运维服务资质（一级）（需提供证明材料并加盖厂商公章） 10.提供三年产品质保和软件升级服务。	2	台

3	全网行为管理	1.网络层吞吐量≥5.8Gb，应用层吞吐量≥750Mb，带宽性能≥500Mb，IPSEC VPN 加密性能≥120Mb，支持用户数≥1000，包转发率≥90Kpps，每秒新建连接数≥10000，最大并发连接数≥500000，标准 1U 设备，内存≥8G，硬盘容量≥128GB MSATA，单电源，接口：≥6 千兆电口。 2.支持网关模式、路由模式、网桥模式、网桥模式（多路桥接模式）和旁路模式等多种模式的网络部署方式，支持电口 bypass。 3.★支持设备利用终端的 MAC 地址作为认证检验值,支持在终端管理列表批量绑定设备 IP/MAC 快捷放通入网。（需提供证明材料并加盖厂商公章） 4.★设备内置海量预分类的 URL 地址库，能够针对各种 URL 类型做识别和分类，同时所有 URL 类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制。（需提供证明材料并加盖厂商公章） 5.★支持多种外联场景检测,例如双网卡场景、无线网卡场景、4G 网卡场景、非法 WIFI 场景，检测到后立刻进行断网操作以及向管理员告警，并弹窗提示终端上网人员。（需提供证明材料并加盖厂商公章） 6.支持针对终端设置访问地址黑白名单,写入终端 ACL 策略,实现强访问管控。 7.支持全网终端资产测绘，提供大屏可视化，可根据 IP 地址段展示全网终端上线情况、IP 地址、Mac 地址以及活跃时间等等。 8.★所投产品具备中国网络安全审查技术与认证中心 CCRC《IT 产品信息安全认证证书》（需提供证明材料并加盖厂商公章） 9.★产品生产厂商为国家标准《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。（需提供证明材料并加盖厂商公章） 10.提供三年产品质保和软件升级服务。	2	台

4	服务器边界防火墙	1.网络层吞吐量≥4G，应用层吞吐量≥2G，防病毒吞吐量≥600M，IPS 吞吐量≥600M，全威胁吞吐量≥450M，并发连接数≥200 万，HTTP 新建连接数≥6 万，IPSec VPN 最大接入数≥300，IPSec VPN 吞吐量≥270M，标准 1U 设备，内存≥4G，硬盘容量≥128G SSD，单电源，接口：≥8 千兆电口+2 千兆光口 SFP。 2.产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求，支持旁路模式。 3.支持独立的入侵防护规则特征库，规则库支持根据漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等进行分类，特征总数在 10000 条以上，能对常见漏洞进行安全防护。 4.支持独立的 WAF 防护模块，WAF 防护特征总数在 4500 条以上，支持针对地址、应用设置 WAF 白名单，支持攻击规则搜索以及自定义。 5.支持服务器抗恶意扫描功能，产品针对扫描源 IP 进行日志记录，并对恶意源 IP 联动封锁。 6.支持基于信誉的僵尸网络防护能力，具备可以持续升级的信誉库，当前僵尸网络信誉库超过 120 万种。 7.★支持 IPSecVPN 链路优化功能，在高丢包场景下，依然保障业务流畅访问体验。（需提供证明材料并加盖厂商公章） 8.支持多对一、一对多和一对一等多种地址转换方式。 9.★支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口，提高链路带宽和链路可靠性。（需提供证明材料并加盖厂商公章） 10.★所投产品厂商应具有国家信息安全漏洞库（CNNVD）技术支撑单位等级证书(一级)。（需提供证明材料并加盖厂商公章） 11.★所投产品的生产厂商需参与制定《信息安全技术 第二代防火墙安全技术 要求》。（需提供证明材料并加盖厂商公章） 12.提供三年产品质保和软件升级服务。	2	台

5	专网边界防火墙	1.网络层吞吐量≥3G，应用层吞吐量≥1G，防病毒吞吐量≥500M，IPS 吞吐量≥400M，全威胁吞吐量≥300M，并发连接数≥100 万，HTTP 新建连接数≥3 万，IPSec VPN 最大接入数≥200，IPSec VPN 吞吐量≥200M，标准 1U 设备，内存≥4G，硬盘容量≥64G SSD，接口：≥6 千兆电口+2 千兆光口 SFP。 2.产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求，支持旁路模式。 3.支持独立的入侵防护规则特征库，规则库支持根据漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等进行分类，特征总数在 10000 条以上，能对常见漏洞进行安全防护。 4.支持独立的 WAF 防护模块，WAF 防护特征总数在 4500 条以上，支持针对地址、应用设置 WAF 白名单，支持攻击规则搜索以及自定义。 5.支持服务器抗恶意扫描功能，产品针对扫描源 IP 进行日志记录，并对恶意源 IP 联动封锁。 6.支持基于信誉的僵尸网络防护能力，具备可以持续升级的信誉库，当前僵尸网络信誉库超过 120 万种。 7.★支持 IPSecVPN 链路优化功能，在高丢包场景下，依然保障业务流畅访问体验。（需提供证明材料并加盖厂商公章） 8.支持多对一、一对多和一对一等多种地址转换方式。 9.★支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口，提高链路带宽和链路可靠性。（需提供证明材料并加盖厂商公章） 10.★所投产品厂商应具有国家信息安全漏洞库（CNNVD）技术支撑单位等级证书(一级)。（需提供证明材料并加盖厂商公章） 11.★所投产品的生产厂商需参与制定《信息安全技术 第二代防火墙安全技术 要求》。（需提供证明材料并加盖厂商公章） 12.提供三年产品质保和软件升级服务。	1	台
6	日志审计	1.默认包含主机审计许可证书数量≥50，最大可扩展审计主机许可数≥150，可用存储量≥2TB，平均每秒处理日志数（eps）最大性能≥2500，标准 2U 设备，内存≥16G，硬盘容量≥128G minisata+2T SATA*2，单电源，接口：≥6 千兆电口+2 万兆光口 SFP+。 2.支持对日志源的批量采集和日志源数据的批量转发。 3.支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用。 4.★支持对单个/多个日志源批量转发，支持定时转发，可通过 syslog 和 kafka 方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志。（需提供证明材料并加盖厂商公章） 5.支持以 FTP 方式将日志数据备份至外部存储空间，支持备份数据的恢复和查询。 6.支持日志检索数据的投屏；支持日志查询结果的统计与导出，支持历史备份文件导入查询。 7.★支持将检索查询的条件收藏为查询模版，支持查询模版创建、导入导出、删除功能，支持历史搜索记录功能。（需提供证明材料并加盖厂商公章） 8.★支持灵活的自定义报表，可以选择模板、数据类型等生成导出报表。（需提供证明材料并加盖厂商公章）	1	台

		9.提供三年产品质保和软件升级服务。		
7	堡垒机	1.默认包含运维授权数≥50，最大可扩展资产数≥150，图形运维最大并发数≥100，字符运维最大并发数≥200，标准1U设备，内存≥8G，硬盘容量≥2T SATA，单电源，接口：≥6千兆电口。 2.支持根据不同应用匹配对应应用登录方式配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入。 3.为防止单一登录认证密码较弱容易被破解的问题，用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD域认证、Radius认证等认证方式;并支持各种认证方式和静态口令组合认证以提升认证强度同时降低被破解盗用的风险。 4.为方便统一管理及分权运维，明确运维分工提升运维效率支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权。 5.★为实现多部门之间业务协同配合实现资源统一调度，支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问。（需提供证明材料并加盖厂商公章） 6.★为提升运维工作与其他业务部门配合满意度，产品支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作。(需提供证明材料并加盖厂商公章) 7.为提升密码复杂度，产品支持密码策略设置，可自定义密码复杂程度，可设置密码中包含数字、字母、符号及禁用关键字等内容。 8.★全面支持IPV6，设备自身可以配置IPV6地址供客户端访问，并且支持目标设备配置IPV6地址实现单点登陆和审计。（需提供证明材料并加盖厂商公章） 9.提供三年产品质保和软件升级服务。	1	台
8	数据库审计	1.最大硬件吞吐量≥2Gbps，最大纯数据库流量≥400Mb/s，数据库实例个数≥30个，SQL处理性能≥30000条SQL/s，日志检索性能≥500000条/秒，标准1U设备，内存≥8G，硬盘容量≥2T SATA，单电源，接口：≥6千兆电口+2万兆光口SFP+。 2.支持包括Redis、MongoDB、Hive、HBaseJavaAPI、kafka、ElasticSearchHttp、ElasticSearchJavaAPI等非关系型数据库。 3.能对已添加的Agent的运行情况进行监控，包括：编号、名称、部署位置、监控的IP地址、操作系统的类型、占用CPU资源以及内存资源情况、运行状态。 4.为保护访问数据安全，支持对日志模糊化处理，防止数据的二次泄密。用户能自定义策略配置，支持风险监控、白名单、黑名单不同策略类型，监控级别能分为高、中、低风险。 5.支持通过首页对全部引擎的审计曲线进行查看，同时支持根据数据库引擎查看单个引擎的审计曲线。且审计曲线支持根据实时、小时、天、周、月的时间维度进行查看。 6.★首页能实时的监控审计设备接收和发送的网络流量，支持对审计设备各网口接收和发送的网络流量进行实时的监控。（需提供证明材料并加盖厂商公章）	1	台

		7.为实现能够给审计设备存储扩容的目的，支持在页面直接配置挂载硬盘。 8.★所投产品具有中国网络安全审查技术与认证中心《中国国家信息安全产品认证证书》。（需提供证明材料并加盖厂商公章） 9.提供三年产品质保和软件升级服务。		
9	WEB 应用防护	1.网络层吞吐量≥4G，应用层吞吐量≥2G，防病毒吞吐量≥600M，IPS 吞吐量≥600M，全威胁吞吐量≥450M，并发连接数≥200 万，HTTP 新建连接数≥6 万，IPSec VPN 最大接入数≥300，IPSec VPN 吞吐量≥270M，标准 1U 设备，内存≥4G，硬盘容量≥128G SSD，单电源，接口：≥8 千兆电口+2 千兆光口 SFP。 2.支持协议深层解析能力,支持应用层 WEB 非加密协议及加密协议流量监测，解析方式包括 XML 格式、JSON 格式解析、伪静态解析等。 3.支持自身内置防护规则库，包含 Web 应用防护规则和 Web 应用漏洞攻击防护规则两种类型，总数量不得低于 6000 种，前者不少于 4800 种，后者不少于 1200 种。 4.★支持通过基于正则表达式自定义 Web 应用防护规则，进而匹配字符串、方向、动作、描述、危险等级、攻击影响等，可以针对多个条件组合，形成深度的 WEB 防护规则。（需提供证明材料并加盖厂商公章） 5.★支持 Web 应用攻击检测防护，支持文件包含攻击、SQL 注入、系统命令注入、XSS、信息泄露攻击、WEBSHELL 后门攻击、跨站请求伪造、目录遍历攻击、WEB 整站系统漏洞等攻击行为。（需提供证明材料并加盖厂商公章） 6.支持使用语义引擎来达到检测不同类型 Web 攻击的目的，使用过程中语义引擎检测功能可单独选择开启或关闭。 7.针对云上黑客入侵，支持自动捕获其 IP 进行防护，并在管理界面一键启用/禁用单个云上黑客 IP。 8.★支持与同品牌安全态势感知产品对接实现相互联动，设备日志等可供安全态势感知产品进行深度分析。（需提供证明材料并加盖厂商公章） 9.★所投产品具备中国网络安全审查技术与认证中心颁发的“Web 应用防护系统”网络关键设备和网络安全专用产品安全认证证书。（需提供证明材料并加盖厂商公章） 10.提供三年产品质保和软件升级服务。	1	台
10	网闸	1.吞吐量≥300Mbps，并发连接数≥10W,标配提供文件交换、数据库访问和同步、视频交换、访问交换等功能模块。标准 2U 设备，“双主机+隔离卡”架构，单主机硬件信息：≥6 千兆电口，内存≥16GB，硬盘≥960G SSD，冗余电源。 2.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。 3.支持对文件内容深度检测，对指定文件的内容关键字过滤，过滤方式至少包括黑白名单设置,确保只有符合保密、安全策略的数据文件才允许被同步，同时可支持文件交换容错和问题告警功能，当文件互传出错时能够自动重传,避免人工干预的同时防止文件丢失,出现异常能够告警提示并记录日志。 4.★支持 Oracle、SQLServer、Mysql、Sybase、DB2、Mariadb、Postgresql 等主流数据库和支持国产人大金仓，南大通用、神舟通用、优炫数据库等数据库的同步。（需提供证明材料并加盖厂商公章） 5.提供任务单独启停控制，避免影响其他数据库同步任务运行。	1	台

		6.★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。（需提供证明材料并加盖厂商公章） 7.★所投产品厂商具有中国信息安全认证中心颁发的信息安全服务资质。（应急处理一级）（需提供证明材料并加盖厂商公章） 8.提供三年产品质保和软件升级服务。		
11	漏洞扫描	1.系统漏扫授权 IP 数≥100，WEB 漏扫授权 URL 数≥20；主机漏扫最大并发 IP 数≥150，WEB 漏扫最大并发 URL 数≥5，标准 1U 设备，内存≥8G，硬盘容量≥128GB SSD+ 2TB SATA，单电源，接口：≥6 千兆电口+2 千兆光口 SFP。 2.支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情。 3.支持从“严重”、“高危”、“中危”、“低危”四个安全级别展示漏洞风险等级的分布情况。 4.★资产发现支持任务立即执行、指定时间执行和周期执行三种执行方式，且指定时间可以精确到分钟，周期执行可精确到每日、每周、每月和自定义周期等。（需提供证明材料并加盖厂商公章） 5.支持认证管理功能，对系统登录信息进行统一管理和配置，提供登录信息的新增、删除和批量导入功能，在系统漏洞扫描和基线核查登录扫描时，可从认证管理中批量导入登录信息。 6.★内置不同的系统漏洞模板，包括高可利用系统漏洞、原理检测系统漏洞、中间件漏洞、数据库漏洞等类型，支持报表形式展示漏洞模板风险等级分布概览，支持报表形式展示漏洞模板详情，包括漏洞总数、漏洞名称、漏洞类型、风险等级等信息。（需提供证明材料并加盖厂商公章） 7.Web 漏洞扫描支持任务立即执行、指定时间执行、周期执行三种执行方式，且指定时间可以精确到分钟，周期执行可精确到每日、每周、每月和自定义周期等。 8.★所投产品厂商应具有中国信息安全认证中心颁发的信息安全服务资质（风险评估一级）。（需提供证明材料并加盖厂商公章） 9.★所投产品厂商应具有国家信息安全漏洞库（CNNVD）技术支撑单位等级证书(一级)。（需提供证明材料并加盖厂商公章） 10.提供三年产品质保和软件升级服务。	1	台

12	安全感知平台	1.网络层吞吐量≥500Mbps，标准1U设备，内存≥16G，硬盘容量≥128G MSATA+4T SATA，单电源，接口：≥6千兆电口+2万兆光口SFP+。 2.展示模块利用人工智能、大数据分析、流量分析、知识图谱等对于网络中的元数据进行深度分析从而检测和威胁分析，产品可以通过大屏展示的形式对网络的整体安全状态进行展示，包括从安全视角对服务器、终端PC进行查看。 3.★大屏展示可以从多个维度对内网安全态势进行展示，例如：安全事件、安全事件趋势、安全事件前5、威胁攻击事件前10、攻击事件类型前5等。（需提供证明材料并加盖厂商公章） 4.产品可以针对最近发生的网络安全热点事件进行可视化展示，并对认可攻击事件进行相关原理的解释，让用户了解内网是否感染力类似病毒，方便及时处置。 5.产品具备勒索病毒的专门检测功能，可以分析出中勒索病毒的主机分布情况、发生趋势，可以通过攻击结果、事件类型、威胁等级、处置状态等进行展示，同时可以结合攻击行为、事件多少进行展示，实现对勒索病毒的实时检测。 6.产品需要支持对于常见的协议进行弱密码检测能力，协议包括WEB、POP3、SMTP、FTP、mysql、LADP等，通过端口镜像流量对业务系统中的弱密码进行检测，实现对于账号、密码、业务系统、IP等信息的检测，并且只有超级管理员有权限查看密码星号。 7.★为了保障告警及时通知到管理员，产品应能够通过微信、短信、邮件的形式进行威胁警告推送，同时推送的频率、时间以及推送的告警条件用户可以自定义，不同的告警可以推送到相应的负责人。（需提供证明材料并加盖厂商公章） 8.★所投产品的生产厂商具备信息技术服务能力，具有ITSS运维符合性证书。（需提供证明材料并加盖厂商公章） 9.提供三年产品质保和软件升级服务	1	台

13	零信任	1.最大加密流量（Mbps）≥300，最大并发用户数≥400，最大 https 并发连接数（个）≥15000，https 新建连接数（个/秒）≥60，标准 1U 设备，内存≥16G，硬盘容量≥128G SSD，单电源，接口：≥6 千兆电口+2 千兆光口 SFP。 2.★为了提高系统可靠性，保障单台设备故障时系统仍可正常运行，综合网关应支持本地集群部署，且最少 2 台设备即可组建集群，单集群的最大节点数量不得少于 4 台；本地集群组建时，集群中的节点可承载工作负载功能，不需要依赖其它外置设备。（需提供证明材料并加盖厂商公章） 3.★为了提升终端用户访问体验，应支持客户端自动选路能力，对于多线路接入场景，支持时延优先的选路模式。（需提供证明材料并加盖厂商公章） 4.为提升业务应用的数据安全性，零信任系统应支持针对发布的 WEB 应用开启 WEB 水印，水印内容至少包括：用户名+当前年月日，起到威慑与溯源作用，有效预防数据泄露。 5.支持帐号密码代填的单点登录功能，支持智能识别登录页面的用户名和密码输入框，根据设置的用户名密码规则自动填写 WEB 业务系统的帐号密码并登录。 6.支持用户在客户端自助进行日志收集，方便运维排查。为了方便快速运维排障，支持管理员在控制台远程获取在线终端的日志，若终端不在线时支持加入排队列表，排队列表中的终端上线后自动收集日志。 7.应支持新增/删除/修改管理员角色，内置审计管理员、安全管理员、系统管理员角色；通过管理员角色配置，实现管理员分级分权。 8.★所投产品的生产厂商具备云安全成熟度模型 CS-CMMI 5 认证。（需提供证明材料并加盖厂商公章） 9.提供三年产品质保和软件升级服务。	1	台
14	安全运营服务	1.提供 7*24 小时运营服务核心资产数≥10。 2.服务方需结合安全工具发现的资产信息，首次进行服务范围内资产的全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP 地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑），并将信息录入到安全运营平台中进行管理。 3.服务正式开始前，需对发现的问题进行处置，避免带病上线；包含内网脆弱性问题，病毒类事件，入侵行为，勒索、挖矿类事件等。 4.需提供不少于每月一次针对服务范围内的资产的系统脆弱性和 Web 漏洞进行全量扫描，并针对发现的脆弱性进行验证。针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案。 5.对发现的脆弱性建立状态总览机制，自动化持续跟踪脆弱性情况，清晰直观地展示脆弱性的修复情况，遗留情况以及脆弱性对比情况，使得招标方可做到脆弱性的可视、可管、可控。 6.策略调配：新增资产、业务变更策略调优服务，业务变更时策略随业务变化而同步更新。 7.支持面向客户的安全态势展示，展示出当前招标方遭受的威胁事件信息以及脆弱性信息统计，并支持服务专家按照资产类别、威胁类型进行定制化筛选查看，能直观感受到客户当前的风险态势情况。（需提供证明材料并加盖厂商公章） 8.服务平台支持面向招标方的安全报告与交付物管理，可生成、导出、下载各类安全报告，包括但不限于《安全服务值守日报》、《特殊时期值守报告》、	1	套

		《安全运营周报》、《安全运营月报》。（需提供证明材料并加盖厂商公章） 9.★所投产品的生产厂商具有信息安全服务资质（安全运营类一级）。（需提供证明材料并加盖厂商公章）		
	合计			

第二、采购实施计划

项目名称：府谷县中医医院网络安全建设服务及设备采购项目

预算金额：984908.00 元；最高限价：984908.00 元

3、采购组织形式：部门集中采购

4、采购方式：竞争性磋商

5、供应商资格条件：

基本资格条件：符合《中华人民共和国政府采购法》第二十二条的规定。

1）供应商应具有独立承担民事责任能力的法人、其他组织或自然人。企业法人应提供合法有效的标识有统一社会信用代码的营业执照（附营业执照的2022 年企业年度报告书）；事业法人应提供事业单位法人证书；其他组织应提供合法登记证明文件；自然人应提供身份证；

2）社会保障资金缴纳证明：提供 2023 年 9 月至投标截止时间已缴纳的至少一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明，单据或证明上应有社保机构或代收机构的公章。依法不需要缴纳社会保障资金的供应商应提供相关文件证明；

3）税收缴纳证明：提供 2023 年 9 月至投标截止时间已缴纳的至少一个月的纳税证明（银行缴费凭证）或完税证明，依法免税的单位应提供相关证明材料；

4）财务状况报告：提供 2022 年度的财务审计报告（至少包括资产负债表、利润表、现金流量表、所有者权益变动表及其附注），公司成立时间不足一年的需提供开标时间前六个月内其基本存款账户开户银行出具的资信证明；

5）信誉要求：供应商在中国政府采购网（www.ccgp.gov.cn）中未被列入政府采购严重违法失信行为记录名单;供应商、法定代表人及项目负责人不得为“信用中国”网站（www.creditchina.gov.cn）中列入重大税收失信主体（提供网站信息查询截图加盖企业原色印章，“信用中国”企业信用信息报告复印件加盖企业原色印章，截图及报告生成时间段为招标文件发出至递交投标文件截止时间内）；供应商、法定代表人及项目负责人不得为中国执行信息公开网（http://zxgk.court.gov.cn）中列入失信被执行人名单（提供网站信息查询截图加盖企业原色印章,截图及报告生成时间段为招标文件发出至递交投标文件截止时间内）；（以采购代理机构谈判现场查询结果为准）；

6）书面声明：参加本次政府采购活动前三年内在经营活动中没有重大违法记录的声明函；

7）提供榆林市政府采购货物类项目供应商信用承诺书及信用中国（陕西榆林）主动承诺网页截图；

8）磋商保证金：用投标信用承诺书代替（提供投标信用承诺书及信用中国（陕西榆林）主动承诺网页截图）；

9）本合同包不接受联合体投标；单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得同时参加本项目投标活动，提供《供应商企业关系关联承诺书》；

6、合同模板

府谷县中医医院网络安全建设服务及设备采购项目

采购合同

甲方：（采购人）

乙方：（供应商名称）

时间：　　年　　月　　日

甲　方：_____

乙　方：_____

依照《中华人民共和国政府采购法》及《中华人民共和国民典法》及有关法规的规定，按照招标程序中标后，遵循平等、自愿、公平和诚实信用的原则，经双方协商，签订本合同并信守下列条款，共同严格履行。

一、货物名称、数量及价格：

编号	名 称	数量		预算投资	
		单位	数量	单价（元）	总价（元）
1	互联网边界防火墙	台	2		
2	入侵防御系统	台	2		
3	全网行为管理	台	2		
4	服务器边界防火墙	台	2		
5	专网边界防火墙	台	1		
6	日志审计	台	1		
7	堡垒机	台	1		
8	数据库审计	台	1		
9	WEB 应用防护	台	1		
10	网闸	台	1		
11	漏洞扫描	台	1		
12	安全感知平台	台	1		
13	零信任	台	1		
14	安全运营服务	套	1		
合计：					

二、交货时间及地点：乙方按照甲方要求，将设备于　　年　　月　　日前送达甲方指定地方。

三、付款方式：

设备安装、调试、培训、验收合格后付合同款95%，剩余5%一年后一次付清。

四、安装及售后服务：

1、乙方负责设备的安装、调试及培训。

2、保修方式：严格按照产品三包服务手册进行三包服务，人为除外。

五、违约责任：

1、乙方违反合同，逾期未完成货物配送任务，乙方承担违约责任，需向甲方支付合同货款总金额5%的违约金。

2、甲方未按合同规定履行付款或者其他义务时，乙方有权追究甲方相应的违约责任。

六、合同争议的解决方式：本合同在履行过程中如发生争议，由双方当事人协商解决，协商不成由任意一方向其所在地法院提起诉讼。

七、合同一式四份，甲乙双方各执二份，自签订之日起生效。

甲方：（盖章）　　乙方：（盖章）

法人代表：（签字）　　法人代表：（签字）

签订日期：　　年　月　日　　签订日期：　　年　月　日

第二、履约验收方案

一、项目概括

1、项目名称：府谷县中医医院网络安全建设服务及设备采购项目

2、该项目计划2024年2月上旬完工。

二、验收小组及成员：由项目分管领导牵头，项目部成立专门验收小组，共同验收。

三、计划验收时间：2024年2月下旬完成采购任务（含质检站强制要求停工时间）。

四、验收程序：

竣工验收：供应商应当严格按合同约定的内容提供服务。采购单位对供应商所提供的货物进行检查确保正常使用，做好验收准备。在供应商履约结束后，验收工作小组按照职责分工对照政府采购合同中验收有关事项和标准核对每项验收事项，并及时组织验收。

五、验收内容及标准：

（一）验收内容

本项目为货物采购，货物数量、规格、质量和参数是否符合相关技术要求。

（二）验收标准

货物数量、规格、质量和参数符合相关技术要求，严格按以下标准验收，并对相关设备进行调试检验以确保其可以正常使用。

六、验收资料的完善归档。

采购单位、采购单位地址、项目联系人及联系电话

1、采购单位：府谷县中医医院

2.采购单位地址：陕西省榆林市府谷县富康路

3.项目联系人：郝主任　　联系电话：13219622889

府谷县中医医院