投标函

1、我公司就 贵州省无线电管理信息系统网络安全建设项目 的 贵州省无线电管理信息系统网络安全建设项目 的 贵州省无线电管理信息系统网络安全建设项目（元）为（大写）： 贰佰陆拾贰万伍仟元整 人民币，小写： 2625000 元 。

2、服务期： 在合同签定后待收到甲方开工令之日起 90 个日历天安装完成建设调试。

3、服务地点： 采购人指定地点

投标函补充内容:

无

供应商名称（盖章）： 联通数字科技有限公司

法定代表人或授权代表： 文韬

地　址： 北京市北京经济技术开发区科谷一街10号院8号楼12层1201（北京自贸试验区高端产业片区亦庄组团）

传　真： 0851-88662086

邮　编： 550081

日　期： 2025年08月07日

一、政府采购报价一览表

1.1.主节点报价一览表

供应商名称(盖章)：联通数字科技有限公司

项目编号：P52000020250006JB

项目名称：贵州省无线电管理信息系统网络安全建设项目　　单位：（元）

序号	内容	投标报价
1	2 台核心交换机，单台配置：1、三层以太网交换机， ≥4U 机架式设备，双主控，双电源，≥24 千兆电口， ≥24 千兆光口， ≥8 万兆光口，业务板插槽≥3；2、交换容量≥20.8Tbps ，IPv4 包转发率≥2880Mpps，包含 3 年硬件质保服务。	98000
2	2 台汇聚交换机，单台配置：1、交换容量≥2.56Tbps ， 转发率≥220Mpps ，MAC 地址表≥32K，路由表容量≥16K ，ARP≥16K；2、接口： ≥8 千兆电+14 万兆光口；3、支持 OAM(802.1AG ， 802.3AH)以太网运行、维护和管理标准；4、支持最大 9 台设备虚拟化；最大堆叠带宽≥160G；5、支持 OPENFLOW 1.3 标准支持普通模式和 Openflow 模式切换，支持多控制器（EQUAL 模式、主备模式）；6、支持 IPv4 静态路由、 RIP V1/V2 、OSPF 、BGP 、ISIS；支持 IPv6 静态路由、RIPng、OSPFv3、BGP4+，支持 IPv4 和 IPv6 环境下的策略路由；7、支持 VRRPv2/v3 （虚拟路由冗余协议）；支持 RRPP （快速环网保护协议），环网故障恢复时间不超过 200ms。	28000
3	1 套超融合软件。性能要求：配置 6 颗 CPU 超融合软件授权，包含管理平台、计算虚拟化、网络虚拟化、存储虚拟化等虚拟化软件。功能要求： 一、云管理平台软件 1、超融合管理系统云管平台软件属于自主研发产品，拥有自主知识产权；管理系统可部署虚拟安全产品，采用完全分布式架构构建，包括计算、存储、网络及云管；*2、对退役服务器的数据自动迁移至其它正常服务器节点；超融合管理系统可部署虚拟安全产品（包括分布式防火墙、下一代防火墙、WAF、负载均衡、数据库审计、 VPN、堡垒机、基线核查、日志审计、终端杀毒等） 采用具有自主知识产权产品，非使用第三方 OEM 产品，保证良好的兼容性和扩展性；3、支持一键大屏显示功能，方便监控集群状态，展示内容包括集群整体拓扑展示、健康状态、资源统计、资源负载情况及告警信息， CPU、内存、存储及网络使用率可以通过 TOP5 方式进行展示；4、支持基于 Web 界面快速扩容计算和存储节点，通过扫描主机或者手动添加的方式增加主机， 扩大集群功能， 支持基于界面自定义物理主机角色， 角色包括计算角色、数据角色、接入角色；5、支持自动化任务功能配置，可以自定义任务类型及执行策略，任务类型包括卷备份和集群巡检等，提升管理效率。二、服务器虚拟化 1、支持主机高可用性功能（HA），当集群中的服务器节点发生故障时，该主机上的虚拟机可以自动在集群内的其它物理机上恢复运行；2、支持虚拟机计算资源自动扩展功能，根据计算资源负载情况实现 CPU 和内存的自动扩展，无需人工干预，提升效率；支持虚拟机级别副本设置， 可以按照业务的安全需求给不同虚拟机设置不同数量副本，提升灵活性；3、支持通过 VNC 和 Spice 两种方式远程访问虚拟机控制台，支持 Spice 方式设置独立访问密码，保证访问安全性；4、支持虚拟机最后一屏功能，指在发生意外故障导致的虚拟机停机，可以将虚拟机最后一屏信息进行截图， 为后续排错提供依据；5、支持 CPU 基准配置，实现同一集群内的异构 CPU 配置，集群中虚拟机可以在不同配置 CPU 的服务器上实现在线的迁移，提供更高的兼容性。三、存储虚拟化 1、采用分布式的软件定义存储架构，且分布式存储属于自主研发产品， 具有自主知识产权， 不能使用开源分布式存储或基于开源分布式存储（如 Glusterfs 、Ceph 等）二次开发的产品；2、支持集群服务器节点数量、服务器磁盘在线扩容，支持磁盘退役功能， 被设置为退役的硬盘， 数据自动迁移到集群其它服务器节点磁盘中；3、支持 2 个或以上多副本冗余技术实现数据高可用性；分布式存储通过多副本冗余技术实现数据高可用性， 支持基于存储卷级别的副本设定， 可以针对不同场景灵活配置不同级别的副本数，最小支持 1 副本，最高支持 6 个副本，副本实现跨磁盘、跨节点、跨机架放置模式；4、超融合不仅支持文件存储、块存储，还应同时支持对象存储服务，可以向外部系统提供对象存储服务， 支持 S3 及 Swift 接口类型，支持 SSL 加密传输，满足非结构化数据存储需求，减少存储额外开支；同时支持存储的 QoS 设置。四、网络虚拟化 1、支持链路聚合满足网络故障切换和负载均衡能力；支持本地网络功能， 通过划分不同的虚拟网络交换机和虚拟端口组进行网络规划，支持端口镜像功能；2、支持实时监控业务可用性，对网络进行监控分析，对指定网络进行流量、协议及端口监控；支	340000

序号	内容	投标报价
	持本地网络功能，通过划分不同的虚拟网络交换机和虚拟端口组进行网络规划， 支持端口镜像功能；3、支持网络监控与分析功能，可以对指定网络进行流量、协议及端口监控，支持规则定义、信息过滤等， 提供完整流量分析功能；4、支持链路探测功能， 可自定义源端和目标端， 支持网络 IP、端口等参数的检测，方便网络排错；5、支持可视化网络功能，网络功能通过软件定义形成独立的网元，包括虚拟交换机、虚拟路由器及虚拟出口等， 可以通过鼠标拖拽网元及连线的方式构建可视化网络， 实现网络环境的快速化构建。	
4	2 台超融合硬件，单台配置：CPU：2 颗处理器，主频不小于 2.0GHz，物理核数不小于 32 核；内存：不小于 256GB DDR4；固态硬盘：不小于 2 块 480GB 企业级固态硬盘；固态缓存盘：不小于 1.92TB 固态缓存盘；机械硬盘：不小于 40TB 企业级硬盘；网卡：超融合集群单个硬件节点至少需要配置 4 个万兆网口以及 4 个千兆网口。	220000
5	6 台接入交换机。单台配置：1、24*10/100/1000BASE-T 电口+4*1G/10G BASE-X SFP+端口；2、交换容量≥672Gbps ，IPv4 包转发率≥126Mpps，包含 3 年硬件质保服务；3、支持 XModem/FTP/TFTP 加载升级，支持命令行接口（CLI），Telnet ，Console 口进行配置，支持 RMON （RemoteMonitoring）告警、事件、历史记录,支持电源的告警功能，风扇、温度告警，支持系统日志，分级告警，调试信息输出；4、支持 GE 端口聚合,支持 10GE 端口聚合，支持静态，动态聚合，支持跨设备聚合；5、支持 IEEE802.3x 流量控制（全双工），支持基于端口速率百分比的风暴抑制，支持基于 PPS 的风暴抑制，支持基于 bps 的风暴抑制；6、支持 32k MAC 地址，支持黑洞 MAC 地址，支持设置端口 MAC 地址学习最大个数；7、支持分布式设备管理， 分布式链路聚合， 分布式弹性路由，支持通过标准以太网接口等方式进行堆叠， 支持本地堆叠和远程堆叠；8、支持 L2（Layer 2）~L4（Layer 4）包过滤功能，提供基于源 MAC 地址、目的 MAC 地址、源 IP(IPv4/IPv6)地址、目的 IP(IPv4/IPv6)地址、TCP/UDP 端口号、VLAN 的流分类，支持入方向和出方向的双向 ACL 策略，支持报文重定向，支持灵活的队列调度算法，可以同时基于端口和队列进行设置，支持 SP、WRR 、WFQ 、SP+WRR 四种模式；9、支持用户分级管理和口令保护，支持 802.1X 认证/集中式 MAC 地址认证，支持端口隔离，支持端口隔离，支持动态 ARP 检测，防止中间人攻击和 ARP 拒绝服务，支持 uRPF(单播反向路径检测)，杜绝 IP 源地址欺骗，防范病毒和攻击。	48000
6	2 台防火墙（核心产品），单台配置：性能要求： 国产化 CPU， 国产化操作系统，冗余电源， ≥6 个千兆电口， ≥4 千兆光口（含多模模块）， ≥2 个万兆光口（含多模模块）； 整机吞吐量≥15G,应用层吞吐量≥12G,最大并发连接数≥400 万,新建连接数≥30 万。 1 个接口扩展槽位，4T 机械硬盘；包含 3 年硬件质保服务， 3 年攻击防护特征库升级。功能要求：1、支持日志外发至多个 SYSLOG 服务器，可设置日志传输协议、外发时间类型、日志语言、合并传输、加密传输等参数；2、支持路由、交换、虚拟线、Listening、混合工作模式；3、支持与本次项目配置的安全管理系统实现协同联动；4、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；5、★支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源， 提高访问效率， 同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（提供截图证明材料并加盖原厂公章）；6、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、邮件安全、数据过滤、文件过滤、审计、 APT 等功能配置,简化用户管理；7、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，可在 WEB 界面显示检测结果；8、支持 IPv4/IPv6 双栈工作模式，支持 RADVD、ND、RIPng、OSPFv3、BGP4+；9、支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回；10、支持对国产主流数据库应用、P2P、移动应用、下载软件加密流量、远程控制软件、工控物联网协议进行识别控制， 支持自定义应用特征；11、支持独立的入侵防护规则特征库， 能对常见漏洞进行安全防护，兼容国家信息安全漏洞库；12、支持行为分析功能，对会话、流量等数据进行统计分析，建立业务行为基线，对异常行为进行告警；13、支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御；14、支持自定义 URL 分类和地址，支持 URL 黑/白名单，支持自定义阻断页面；15、支持文件过滤，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM 文件传输等应用类型以及 HTTP/FTP/SMTP/POP3 等标准协议进行检测 16、支持内容过滤， 如 FTP 上传文件、下载文件、删除文件或文本、重命名、创建目录、删除目录、显示文件列表等；17、★产品具备信息安全产品自主原创证明证书。	180000

序号	内容	投标报价
7	2 台病毒过滤网关/防毒墙，单台配置：性能要求：国产化 CPU，国产化操作系统，机械硬盘≥4T；≥6 个千兆电口（含 2 对 bypass）， ≥4 个千兆光口（含多模模块），4 万兆光口（含多模模块）,冗余电源,1 个扩展槽位,整机吞吐率≥15Gbps，最大并发连接数 800W，病毒检测吞吐率≥5Gbps；包含 3 年硬件质保服务， 3 年特征库升级服务。功能要求： 1、★设备必须为专业的防病毒网关产品，非防火墙/下一代防火墙、UTM、IPS 等具有防病毒功能模块的产品（提供产品 web 管理主界面截图并加盖原厂公章）2、支持双引擎双库，且两个引擎可同时工作，各个应用协议可分别选择使用不同的病毒扫描引擎（快速扫描引擎或深度扫描引擎）进行病毒检测；3、能够防御病毒、木马、蠕虫、间谍软件等恶意软件，且支持对压缩数据、加壳病毒的检测与处理；4、支持对 HTTP、FTP、POP3、 SMTP、IMAP 等常用应用协议进行病毒检测与过滤；5、病毒引擎具备自动化的数据解压缩能力，无需手动配置，具备 64 层的数据解压缩病毒检测能力；6、支持联动态势感知探针产品，识别未知病毒，防御 APT 攻击；7、支持 IPv6、IPv6 over IPv4、IPv6 和 IPv4 混合网络， 能够在该网络环境中检测出病毒流量；8、流行病毒检测率不低于 95%，并提供国家专业病毒检测机构的证明；9、病毒网关默认加载的流行病毒库总数大于 2000 万，可本地化完成病毒地检测过滤与处理，无需发送到云端检测；10、支持 IP、ICMP、TCP、UDP、HTTP、HTTPS、SIP、NTP、DNS 等协议的 DDoS 攻击防御；11、支持多条链路的即插即用病毒检测防御模式， 可利用同一台病毒过滤网关实现多链路防护， 增强业主单位网络安全性并节省业主单位的病毒防御成本；	188000
8	2 台核心业务域防火墙，单台配置：性能要求：≥4T 机械硬盘；交流冗余电源；≥6 个千兆电口、≥4 个千兆光口、≥4 个万兆光口（满配万兆多模模块；支持 IPS、防病毒、应用控制、 IPSec VPN、SSL VPN 等功能；网络吞吐≥40Gbps，应用吞吐≥32Gbps，最大并发连接≥1200 万，包含 3 年硬件质保服务， 3 年攻击防护、病毒过滤特征库升级。功能要求：1、支持日志外发至多个 SYSLOG 服务器，可设置日志传输协议、外发时间类型、日志语言、合并传输、加密传输等参数；2、支持路由、交换、虚拟线、 Listening、混合工作模式；3、支持与本次项目配置的安全管理系统实现协同联动。4、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；5、支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源， 提高访问效率， 同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡；6、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、邮件安全、数据过滤、文件过滤、审计、 APT 等功能配置,简化用户管理；7、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,可在 WEB 界面显示检测结果;8、支持 IPv4/IPv6 双栈工作模式,支持 RADVD、ND、RIPng、OSPFv3、BGP4+；9、支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回；10、支持对国产主流数据库应用、P2P、移动应用、下载软件加密流量、远程控制软件、工控物联网协议进行识别控制， 支持自定义应用特征；11、支持独立的入侵防护规则特征库， 能对常见漏洞进行安全防护，兼容国家信息安全漏洞库；12、支持行为分析功能，对会话、流量等数据进行统计分析，建立业务行为基线，对异常行为进行告警；13、支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御；14、支持自定义 URL 分类和地址，支持 URL 黑/白名单，支持自定义阻断页面；15、支持文件过滤，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM 文件传输等应用类型以及 HTTP/FTP/SMTP/POP3 等标准协议进行检测 16、支持内容过滤， 如 FTP 上传文件、下载文件、删除文件或文本、重命名、创建目录、删除目录、显示文件列表等；	246000

序号	内容	投标报价
9	1 台 Web 应用防护，配置要求：性能要求：≥4 个 千兆电口、≥4 个千兆光口（含多模模块）、≥2 个万兆光口（含多模模块）； 32G 内存，4T 硬盘；冗余双电源；HTTP 吞吐： ≥15Gbps； HTTP 新建（CPS）： ≥120,000/s；HTTP 最大并发连接数： ≥400 万；含网页防篡改功能，包含 3 年硬件质保服务， 3 年特征库升级服务。功能要求：1、支持无 IP 纯透明模式串联部署、负载均衡模式部署、反向代理模式部署、旁路监测模式部署。2、支持虚拟线接入，无论任何网络环境可强制数据从一个接口转发到另一个接口 3、支持对 HTTP 协议合法性进行验证， 支持对 HTTP 协议的 URI 、 HOST 、 UA 、 Cookie 、 Referer 、 Content 、 Accept、Range、其他头部和参数在内的元素、参数进行检测与处理。且支持非法编码和解码的灵活控制与处理；4、支持针对主流 Web 服务器及插件的已知漏洞防护， Web 服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS 等插件应覆盖 :dedecms 、phpmyadmin 、PHPWind 、 shopex、discuz、ecshop、vbulletin、wordpress 等，提供 Java 反序列化漏洞（Jboss）防护规则；5、支持 HTTP 访问控制功能，可以提供针对 HTTP 元素和客户端的组合访问控制策略。支持对多种 HTTP 方法执行访问控制，包括：GET、POST、HEAD、PUT、DELETE、MKCOL、COPY、MOVE、OPTIONS 、 PROPFIND 、 PROPPATCH 、 LOCK 、 UNLOCK TRACE 、SEARCH、CONNECT；6、扫描防护:攻击者通常会利用各种工具扫描网站， 探测网站漏洞，给网站的安全带来极大隐患。 WAF 可以通过识别扫描工具的数据特征值， 阻断扫描工具的探测。支持基于请求量统计和应答分布统计等算法对扫描行为进行分析并防护；7、人机识别:可通过 JS 脚本识别自动化工具，并能够对自动化工具访问请求配置放过、阻断、接受、伪装等处置动作。可以根据客户端环境检测， 识别攻击工具， 主要包括市面上主流扫描器，如 burpsuite、nessus 等，市面上主流自动化工具 selenium、phantomjs 等的脚本攻击识别；	96000
10	1 台数据库审计，配置要求：性能要求： ≥6 个千兆电口， 4 个千兆光口（含多模模块），≥2 个万兆光口（含多模模块）， 硬盘 :2TB； 1 个扩展槽;2 个 USB,1 个 CONSOLE 口 ；双电源;峰值入库速度:18000（条/秒）,无实例数限制,网络吞吐≥5G,SQL 吞吐≥1000M。默认 3 年硬件质保服务。功能要求： 1、对无法镜像流量的审计场景，支持多种类型操作系统的探针部署，适配的操作系统至少包括常见操作系统、国产操作系统 2、支持细粒度解析数据库协议，包括关系型数据库、国产化数据库等。3、支持 HTTP、Telnet、FTP、Rlogin 的审计 4、具备数据库操作类、表、视图、索引、触发器、游标、事务各种对象的 SQL 操作审计 5、支持数据库请求和返回的双向审计,特别是 SQL 返回结果集、SQL 语句响应时间、连接时长、表影响的字段、影响行数等内容 6、支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址、端口、发现时间、会话时长、总事件数等信息， 并且自动添加到待监控审计列表，无需用户提供网段、数据库地址等信息。7、支持依据数据库实例监控各个数据库的连接池、缓冲区、表空间、死锁、CPU、内存、硬盘等信息，可自定义告警阈值进行健康评估 8、支持数据库服务器弱口令扫描，扫描出的弱密码支持脱敏显示 9、支持对针对数据库的 XSS 攻击行为、 SQL 注入攻击行为，利用漏洞攻击等行为进行审计，内置审计规则不需要额外配置，并进行实时报警；10、支持以用户名、源 IP、部门、域名、主机名、邮箱、联系电话为条件的实名审 11、支持基于数据库时间、源/目的 IP、数据库名、应用协议、数据库表名、字段值、预处理 SQL、SQL 语句、SQL 返回结果集、返回码、SQL 语句响应时间、SQL 操作类型、影响行数等条件的审计查询。12、支持超长 SQL 语句审计，至少不低于 2M，支持多层嵌套 SQL 语句的审计， 有效分割、准确审计主流数据库协议的多 SQL 语句	66000

序号	内容	投标报价
11	1台全威胁检测系统，配置要求：性能要求：机械硬盘≥1TB，≥6 个千兆电口，≥4 个千兆光口（含多模模块）， ≥2 万兆光口（含多模模块），冗余电源,4 个扩展槽位,最大并发连接数： ≥800W，综合威胁检测能力： ≥10Gbps。含：3 年攻击检测规则库、应用识别库、地理信息库、僵尸主机规则库、威胁情报库、URL 分类库升级许可。包含 3 年硬件质保服务功能要求： 1、★支持全流量取证，将事件发生前后的流量一起留存，支持攻击取证、僵尸主机取证、恶意程序样本、威胁情报取证，取证类型支持报文取证和样本文件取证两种形式。（（提供截图证明材料并加盖原厂公章））2、支持对设备进行网络参数配置，包括长连接占总连接的百分比、握手时 TCP 连接超时、TCP 超时时间、其他连接超时、 TCPReset、连接完整、只允许 SYN 报文建立新连接、长连接超时、关闭时 TCP 超时时间、UDP 超时时间、校验和检查、分片重组、快速连接重用等参数。3、支持在线抓包，可配置抓包数量、协议类型、源 IP、源端口、目的 IP、目的端口、源或目的 IP、源或目的端口、文件名、接口、 VLAN ID 等。支持在线多任务并行抓包 4、Syslog 支持配置多个服务器地址， 支持 TCP、UDP 传输协议，支持 UTF8、GB2312 编码格式，支持选择是否以加密方式传输，可选择证书加密或密码加密。5、支持独立的攻击检测引擎， 支持 9700 种以上的攻击规则库。6、支持能够检测包括扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、非授权访问、注入攻击、 URL 跳转、跨站攻击、 WebShell、浏览器劫持、文件漏洞攻击、工控漏洞攻击、物联网漏洞攻击等在内的 16 大类超过 9700 种以上网络攻击事件，支持多种常见攻击行为进行检测。7、支持自定义规则，并且自定义规则库可以导入导出。8、★支持服务器非法外联检测， 支持按 IP 地址、IP 范围、子网设置监测对象，支持仅对外联境外地址监测，支持按 IP 地址、IP 范围、子网设置外联白名单。支持对服务器外联行为自学习， 自动记录外联信息，包括 IP 地址、协议、端口/ICMP 类型、连接数。（提供截图证明）可设置相应警告、联动阻断动作。（提供截图证明并加盖原厂公章）9、支持独立的 DDoS 检测引擎，支持对 IP 扫描攻击、端口扫描攻击等多种扫描攻击行为检测；10、支持对恶意程序实现特征检测、机器学习检测、内置虚拟沙箱检测等多种检测方式， 并且多种检测方式相互独立、互不影响，可对检测到的恶意文件设置相应警告、联动阻断动作；支持专业沙箱设备联动检测。11、支持通过威胁情报检测已知 APT 事件，通过恶意程序检测未知 APT 事件，通过僵尸行为规则库检测已知的 APT 组织。12、支持对 SQL 注入攻击、跨站攻击、浏览器劫持攻击、URL 跳转攻击、WEB 远程代码执行攻击、 WEB 缓冲区溢出攻击、 WEB 漏洞攻击、Webshell 上传攻击、WEB 越权攻击、WEB 扫描攻击、目录遍历攻击、WEB 口令暴力破解攻击等多种类型的 WEB 攻击检测。13、本地嵌入独立的威胁情报库， 不依赖其他设备或情报平台，即可独立的实现威胁情报检测能力，可对检测到的恶意文件、恶意 IP/域名、恶意 URL 设置相应捕获、联动阻断动作。14、支持卸载 SSL， 实现对 HTTPS、IMAPS、SMTPS、POP3S、FTP、RDP、MQTT、SIP 等加密流量的分析检测。15、支持数量超过 1000 万的 URL 分类库，URL 类型涉及包括搜索引擎、网上购物、社交网络、求职招聘、财经、下载、政策法规、成人内容、非法及不良等。	86000
12	1台网络准入控制设备，配置要求：性能要求： ≥6 个千兆电口，终端授权支持扩容≥5000 点；本次项目配置≥400 点终端授权。三年硬件质保。功能要求： 1、支持双操作系统冷备、双机热备，在单机模式下，提供独立系统逃生工具。2、支持策略路由、端口镜像、透明网桥、 802.1X 、ARP、DHCP、VLAN 隔离、Portal 等准入技术，支持准入技术自由组合使用，满足各种复杂网络环境；3、支持划定关键业务范围，针对终端用户发起的访问请求可强制要求二次认证校验；4、能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP 表等信息；支持在界面上提供对该网络设备进行 TELNET、SSH 等管理；能够在网络拓扑图上由用户自定义显示的节点类型，方便用户通过不同方式查看拓扑连接；5、支持设置来宾专属地址段；来宾入网提供二维码、来宾码、自助申请（管理员审批）多种方式；提供来宾入网审批气泡弹窗提醒功能，被访人点击即可审批；6、移动终端可以支持通过将指纹和用户账户绑定的方法，实现用户按压指纹认证入网；7、软件、消息分发：支持基于部门、角色（分组）、设备或 ip 段进行软件、消息分发， 分发周期支持立即、每天、每周、每月等周期设置。针对分发的源文件支持设置保留或不保留， 分发后支持重启或关闭计算机；8、在无客户端的方式下，可发现终端同时连接内网和外网的行为，在外网违规外联服务器上能够查看到违规外联条目信息；针对违规外联的终端能够阻断起内网连接；	86000

序号	内容	投标报价
13	1 台运维安全审计，配置要求：性能要求：≥6 个千兆电口；≥2TB 硬盘，交流冗余电源；≥ 100 个资产管理授权；包含 3 年硬件质保服务，3 年特征库升级服务。功能要求： 1、支持物理旁路部署，不改变现有网络结构；2、支持第三方证书用户自行上传用作校验的 CA 证书和 CRL 列表；3、本地 CA 支持根证书的重新生成及替换；支持根据根证书签发出客户端证书；支持发布生成吊销列表；支持国密证书认证。4、支持资源分类和资源系统类型管理： 内置常见资源分类和资源系统类型， 可自定义添加资源分类、资源系统类型和资源服务类型 5、支持对已添加的设备账号进行密码托管，从而实现单点登录功能；6、 自动对数据库、Windows、Linux 等设备进行账号改密，改密支持手动和定期任务，密码配置支持全局策略和手工指定，密码复杂度支持按策略随机生成；7、支持按照用户、用户组、资产、资产组、管理协议、资产账号进行一对一、一对多、多对一、多对多授权；8、支持会话、指令、剪切板上下行、文件上传下载的约束行为；9、提供授权关系查看功能， 图形化直观展示用户、资产、协议、账号的授权关系 10、支持会话请求远程协助，且协同会话保持实时同步；7、11、支持全文审计检索。可以对操作行为中的用户信息、资产信息、管理地址信息、管理方式信息、操作命令信息、操作结果信息进行全文检索、过滤， 极大提高查询效率， 更方便的进行用户关联追溯。12、支持自动执行运维脚本。运维脚本分为内置和自定义。13、支持对堡垒机虚拟为多台逻辑堡垒机， 虚拟堡垒机之间实现独立配置、 独立数据。实现 IT 资源的动态分配、灵活调度、跨域共享，提高 IT 资源利用率。14、支持配置数据和审计数据的备份、自动清理， 支持备份数据通过 FTP 方式远程备份；支持磁盘映射手动/自动清理；	56000
14	1 台日志审计设备，配置要求：性能要求：存储空间≥6T 硬盘，32G 内存， ≥4 个千兆电口， 4 个千兆光口（含多模模块），冗余电源；≥8000EPS，200 个管理设备授权；出厂默认 3 年软硬件质保服务。功能要求：2、支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等日志对象的日志数据采集。3、对于尚未支持的设备类型日志进行新增采集支持，在页面上传升级文件或增加配置文件即可；4、支持主动、被动相结合的数据采集方式；支持 Syslog、SNMPTrap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过 Agent 采集日志数据。5、系统内置已支持设备种类清单，提供设备日志外发配置建议指导 6、支持实时自动刷新每个日志源的实时日志列表，支持在实时日志界面通过选择过滤器来监视所关注的特定类型的日志；7、支持首页展示日志采集总量统计，可按不同日志源种类分类显示日志总量及大小，并支持导出；8、支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率， 降低对系统资源的占用， 保障重要日志的收集；9、支持根据设备重要程度独立设置每个被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个月和永久保存等参数；10、支持原始日志全文检索；11、支持在一个日志源查询结果列表中将 IP 作为源地址或目的地址查询条件，直接跳转到其他日志源类型中进行查询；12、系统内置安全知识库， 支持自定义增加安全知识内容， 可在关联分析规则中关联知识。	56000

序号	内容	投标报价
15	1 台态势感知平台（核心产品），配置要求：性能要求： ≥6 个千兆电口，≥2 个万兆光口（含多模模块），冗余电源,1 个扩展槽位,双 CPU，≥256G 内存，≥40TB 硬盘，支持 raid，数据采集器性能≥20000 条/秒；支持 10 亿条数据秒级检索响应。 支持态势监测、响应处置、分析研判、资产管理、集中管控、安全治理、安全审计、威胁情报等功能模块。配置 20 个联动设备接入授权,3 年质保， 3 年系统升级服务功能要求：★1、提供全网态势、威胁态势、资产态势、漏洞态势、攻击态势、恶意程序态势等展示界面（提供截图证明材料并加盖原厂公章）2、支持安全处置功能： 支持告警工单处置人、告警处置结果、未处置状态统计及详情。3、支持漏洞监测功能： 支持联动漏扫设备或手动导入漏扫报告方式实现漏洞数据采集， 支持不同品牌漏扫设备联动， 支持 excel、zip 等类型的漏扫报告导入；4、支持响应编排功能：支持基于场景的安全策略响应编排 5、支持工单管理功能，支持指派相关责任人进行处理，支持对工单进行分组管理，分组类型包括我的工单、待处置工单、已处置工单、历史工单：6、支持资产管理功能：支持资产新增、修改、删除，支持自定义资产信息， 包括资产三性等基本信息、资产类型、所属业务系统、所属物理位置、责任人、漏洞、补丁及软硬件信息等，支持资产批量删除、资产导出、资产导入 7、支持管控设备概览功能：支持通过界面快速添加集中管控设备，★8、支持管控设备拓扑图展示功能：支持拓扑动态提示管理设备产生的告警， 支持拓扑图右击直接查看选中设备的设备概览、设备详情、告警列表等信息， 支持设备策略集中管理功能：包括配置信息、运行配置、配置备份、模块管理、日志外发、升级管理、配置审计，支持日志外发地址、端口、协议配置，支持设备升级的版本号、序列号展示， 支持设备操作记录审计，包括审计时间、配置类型、结果状态、执行设备地址、执行设备名称、执行设备类型、操作人、审计内容等（提供截图证明材料并加盖原厂公章）9、支持设备策略集中管理功能：包括配置信息、运行配置、配置备份、模块管理、日志外发、升级管理、配置审计， 支持日志外发地址、端口、协议配置， 支持设备升级的版本号、序列号展示，支持设备操作记录审计， 包括审计时间、配置类型、结果状态、执行设备地址、执行设备名称、执行设备类型、操作人、审计内容等。10、支持全网策略概览功能：支持下发策略统计、配置备份统计、活跃策略、最新下发策略操作人、最新下发策略设备、最新策略任务、最新配置备份、最新失败审计等监控能力 11、支持多种类型设备策略配置功能：支持多种策略配置，包括但不限于访问控制策略、静态黑名单、动态黑名单、安全策略等 12、支持全部被管设备配置集中审计，支持审计查询，13、支持安全报告功能：包括但不限于安全报告、合规审计日志、应急预案、跟踪文档、待整改业务系统展示， 支持待整改业务系统排名、最新安全报告排名、最新跟踪文档等信息， 最新安全报告支持下载 14、支持应急预案：包括但不限于可疑异常、设备故障、网络攻击、内容安全、有害程序、信息破坏分类；15、支持内生情报管理功能：包括恶意 IP 地址、恶意 URL、恶意样本、恶意域名、垃圾邮件等， 支持情报进行分类自定义查询，支持自定义威胁情报信息，支持威胁情报的导入	120000
16	1 套无线电管理平台防护系统(核心产品)，配置要求：1、配置 1 套无线电管理平台防护系统，实现对无线电管理一体化平台的两个集群进行防护安全防护。 3 年升级服务功能要求：1、采用 Agent-Server 架构，支持通过 B/S 管理方式对主机进行集中管理。2、Agent 运行支持业务优先、均衡模式、防护优先等运行模式，以应满足不同应用场景。3、支持通过管理端对 agent 进行批量启用、停用、卸载、删除、升级和重连，支持按 agent 版本、操作系统版本、agent 状态、在线状态、安装时间等进行搜索。4、★采用 ARP、PING 扫描、NMAP 扫描多种探查方法，主动发现未安装安全探针的主机的信息， 包含 IP 地址、MAC 地址、操作系统、安装状况、最近扫描方式等，支持以模板 xlsx 格式手动导入资产。（提供 CNAS/CMA 资质的第三方测试报告）5、★支持扫描中间件漏洞，包括但不限于 Apache、Nginx、Tomcat，可以扫描 SQL 注入、XSS 跨站点脚本、命令行注入、 CSP 配置漏洞、目录遍历攻击等网站漏洞， 支持查看风险详情， 提供修复建议，支持对操作系统及 MySQL、Redis 等应用的弱密码进行检测，支持字典管理等功能；（提供截图证明材料并加盖原厂公章）6、支持实时检测内核后门、引导后门、勒索病毒、流氓程序、黑客工具等病毒， 检测内容至少包含类型、病毒名称、病毒 ID 等信息，支持隔离、信任、删除、溯源操作。7 、支持检测 SSHD、FTP、RDP 等暴力破解入侵行为， 灵活配置检测策略，包含设置攻击检测周期、攻击次数阈值与处理方式（包含仅记录和记录自动停封），提供白名单和黑名单。8、支持实时检测异常 IP、异常区域、异常时间、异常账号等异常登录行为，展示威胁事件详情，包含主机 IP、登录区域、登录账号、来源、登录时间、异常类型等。9、实时检测 ASP、ASPX、PHP、JSP 等 Webshell 后门，支持隔离、信任、删除、溯源操作。10、实时检测隐藏进程、隐藏端口号进程、子权限大于父权限等异常进程并产生告警，包括异常进程、进程路径、进程 ID、父进程 ID、状态等，支持对异常进程加黑处理 11、实时检测提权行为并产生告警， 告	158000

序号	内容	投标报价
	警信息至少包括被提权主机 IP 地址、发现时间、提权进程、提权用户、进程 ID、父进程 ID 等，支持设置黑名单。12、实时监控系统命令篡改行为， 防止命令注入攻击， 告警信息包括篡改命令、主机 IP 地址、操作路径， 支持设置白名单。13、提供中标麒麟、银河麒麟、 Suse、CentOS、RedHat、 Ubuntu 等操作系统基线模板；Apache、Nginx、Tomcat、Weblogic、Redis、MySQL、DB2 等应用基线，支持提供等保二级、三级主机安全合规检查基线，支持提供 CIS Level1、Level2 基线。	
17	1 台漏扫设备，配置要求：性能要求：1 个 CONSOLE 口，≥2 个 USB 口；≥6 个千兆电口， ≥2 个千兆光口；1T 硬盘； 支持系统扫描，最大可扫描 IP 或域名数无限制，扫描任务并发 5，扫描 IP 并发 80； 支持 Web 扫描； 支持弱口令检测；包含 3 年硬件质保服务， 3 年特征库升级服务。功能要求： 1、支持扫描主流操作系统、 Web 服务器、数据库、网络主机、移动设备、应用及软件的安全漏洞 2、支持 IPv4/IPv6 双协议栈地址场景漏洞扫描 3、支持防火墙联动功能，防火墙能根据漏扫提供的资产信息对重要资产信息进行防护，根据漏洞信息自动生成防护规则，保护内网安全；4、支持外发至 SYSLOG 服务器，可将多条日志合并成一条日志传送到日志服务器中，支持加密传输 5、支持扫描系统漏洞数量大于 240000 种，web 漏洞数量大于 5000 种,数据库大于 3000 种，CVE 漏洞数大于 60000；6、产品漏洞库应涵盖目前的安全漏洞和攻击特征，漏洞库具备至少 CVE、CNCVE、CNVD、BUGTRAQ、CNNVD 编号 7、支持扫描大数据组件的安全漏洞，如 Spark、Splunk、Kafka、Storm、Cassandra、Ambari、Impala、Solr、Oozie、Hbase、Hadoop 等 8、扫描目标支持 ip、域名、网段、子网的组合配置；9、主机存活探测支持 ARP ping、ICMP ping、TCP ping、UDPping、TCP SYN Ping、TCP ACK Ping 等多种方式 10、支持对 DB2、MSSQL、MySQL、Oracle、GBASE、DMDB 等主流数据库进行登陆认证扫描；11、支持站点组、单站点风险在线报表和站点特有属性配置 12、支持排除路径名，可自定义无需爬取的 URL 链接；13、支持主流操作系统配置核查，包括但不限于 Windows、Linux、BClinux、Solaris、HPUnix、AIX 等操作系统，支持中标麒麟、优麒麟、中兴新支点等国产化操作系统 14、支持 Elasticsearch、ZooKeeper、Spark、HDFS、Kafka、HBase、Hive、Sqoop、Yarn-MR、Impala 等大数据组件的配置核查	76000
	合计（元）	2148000
投标总价（人名币大写）：贰佰壹拾肆万捌仟元 投标总价（人民币小写）：2148000 元		
项目完成时间：在合同签定后待收到甲方开工令之日起 90 个日历天安装完成且调试验收合格		
优惠条件及备注：无		

供应商法定代表人或授权代表签字：

职务：客户经理 日期：2025 年 8 月 07 日

1.2.备节点报价一览表

供应商名称(盖章)：联通数字科技有限公司

项目编号：P52000020250006JB

项目名称：贵州省无线电管理信息系统网络安全建设项目　　单位：（元）

序号	内容	投标报价
1	1 台核心交换机，单台配置：1 、标准配置：三层以太网交换机， ≥4U 机架式设备，双主控,双电源,≥24 千兆电口,≥24 千兆光口,≥8 万兆光口;2、交换容量≥20.8Tbps，IPv4 包转发率≥2880Mpps，包含 3 年硬件质保服务。	46000
2	1 台防火墙，性能要求：国产化 CPU，国产化操作系统，冗余电源，≥6 个千兆电口， ≥4 千兆光口（含多模模块）， ≥2 个万兆光口（含多模模块）； 整机吞吐量≥15G,应用层吞吐量≥12G,最大并发连接数≥400 万,新建连接数≥30 万。1 个接口扩展槽位，4T 机械硬盘；包含 3 年硬件质保服务，3 年攻击防护特征库升级。功能要求：1、支持日志外发至多个 SYSLOG 服务器，可设置日志传输协议、外发时间类型、日志语言、合并传输、加密传输等参数；2、支持路由、交换、虚拟线、 Listening、混合工作模式；3、支持与本次项目配置的安全管理系统实现协同联动。4、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；5、支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡；6、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、邮件安全、数据过滤、文件过滤、审计、APT 等功能配置,简化用户管理；7、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，可在 WEB 界面显示检测结果;8、支持 IPv4/IPv6 双栈工作模式， 支持 RADVD、ND、RIPng、OSPFv3、BGP4+；9、支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回；10、支持对国产主流数据库应用、 P2P、移动应用、下载软件加密流量、远程控制软件、工控物联网协议进行识别控制，支持自定义应用特征；11、支持独立的入侵防护规则特征库，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库；12、支持行为分析功能，对会话、流量等数据进行统计分析，建立业务行为基线，对异常行为进行告警；13、支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御；14、支持自定义 URL 分类和地址，支持 URL 黑/白名单，支持自定义阻断页面；15、支持文件过滤，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM 文件传输等应用类型以及 HTTP/FTP/SMTP/POP3 等标准协议进行检测 16、支持内容过滤，如 FTP 上传文件、下载文件、删除文件或文本、重命名、创建目录、删除目录、显示文件列表等；	90000
3	1 台日志审计，性能要求：存储空间≥6T 硬盘，32G 内存，≥4 个千兆电口，4 个 SFP 插槽（含多模模块），冗余电源；8000EPS，200 个管理设备授权；出厂默认 3 年软硬件质保服务。功能要求：2、支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等日志对象的日志数据采集。3、对于尚未支持的设备类型日志进行新增采集支持， 在页面上传升级文件或增加配置文件即可；4、支持主动、被动相结合的数据采集方式；支持 Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过 Agent 采集日志数据。5、系统内置已支持设备种类清单，提供设备日志外发配置建议指导 6、支持实时自动刷新每个日志源的实时日志列表， 支持在实时日志界面通过选择过滤器来监视所关注的特定类型的日志； (7、支持首页展示日志采集总量统计， 可按不同日志源种类分类显示日志总量及大小，并支持导出；8、支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集；9、支持根据设备重要程度独立设置每个被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个月和永久保存等参数；10、支持原始日志全文检索；11、支持在一个日志源查询结果列表中将 IP 作为源地址或目的地址查询条件，直接跳转到其他日志源类型中进行查询；12、系统内置安全知识库，支持自定义增加安全知识内容，可在关联分析规则中关联知识。	68000

序号	内容	投标报价
4	1 台数据库审计设备，性能要求：≥6 个千兆电口，4 个千兆光口（含多模模块），≥2 个万兆光口（含多模模块），硬盘:2TB；1 个扩展槽;2 个 USB,1 个 CONSOLE 口 ;双电源；峰值入库速度:18000（条/秒） ;无实例数限制，网络吞吐≥5G,SQL 吞吐≥1000M。3 年硬件质保服务。功能要求：1、对无法镜像流量的审计场景，支持多种类型操作系统的探针部署，适配的操作系统至少包括常见操作系统、国产操作系统 2、支持细粒度解析数据库协议， 包括关系型数据库、国产化数据库等。3、支持 HTTP、Telnet、FTP、Rlogin 的审计 4、具备数据库操作类、表、视图、索引、触发器、游标、事务各种对象的 SQL 操作审计 5、支持数据库请求和返回的双向审计，特别是 SQL 返回结果集、SQL 语句响应时间、连接时长、表影响的字段、影响行数等内容 6、支持从数据库流量中自动识别数据库， 从流量分析结果中自动判别包含的数据库类型、版本、地址、端口、发现时间、会话时长、总事件数等信息，并且自动添加到待监控审计列表，无需用户提供网段、数据库地址等信息。7、支持依据数据库实例监控各个数据库的连接池、缓冲区、表空间、死锁、 CPU、内存、硬盘等信息， 可自定义告警阈值进行健康评估 8、支持数据库服务器弱口令扫描， 扫描出的弱密码支持脱敏显示 9、支持对针对数据库的 XSS 攻击行为、SQL 注入攻击行为，利用漏洞攻击等行为进行审计， 内置审计规则不需要额外配置，并进行实时报警；10、支持以用户名、源 IP、部门、域名、主机名、邮箱、联系电话为条件的实名审计 11、支持基于数据库时间、源/目的 IP、数据库名、应用协议、数据库表名、字段值、预处理 SQL、SQL 语句、SQL 返回结果集、返回码、SQL 语句响应时间、SQL 操作类型、影响行数等条件的审计查询。12、支持超长 SQL 语句审计，至少不低于 2M，支持多层嵌套 SQL 语句的审计，有效分割、准确审计主流数据库协议的多 SQL 语句。	75000
合计（元）		279000
投标总价（人名币大写）：贰拾柒万玖仟元 投标总价（人民币小写）：279000 元		
项目完成时间：在合同签定后待收到甲方开工令之日起 90 个日历天安装完成且调试验收合格		
优惠条件及备注：无		

供应商法定代表人或授权代表签字：_____

职务：客户经理 日期：2025 年 8 月 07 日

1.3.集成服务报价一览表

供应商名称(盖章)：联通数字科技有限公司

项目编号：P520000202500006JB

项目名称：贵州省无线电管理信息系统网络安全建设项目　　单位：（元）

序号	内容	投标报价
1	包含软硬件设备的安装、本机调试、联网调试等集成服务内容。	198000
合计（元）		198000
投标总价（人名币大写）：拾玖万捌仟元 投标总价（人民币小写）：198000 元		
项目完成时间：在合同签定后待收到甲方开工令之日起 90 个日历天安装完成且调试验收合格		
优惠条件及备注：无		

供应商法定代表人或授权代表签字：

职务：客户经理　　日期：2025 年 8 月 07 日