兴平市人民检察院网络安全设备购置项目

合同书

采购方：兴平市人民检察院

供应商：陕西奥博迪特电子科技有限公司

2026 年 10 月

合同条款

合同签订地：兴平市

采购方（以下简称甲方）：兴平市人民检察院

供应商（以下简称乙方）：陕西奥博迪特电子科技有限公司

依据《中华人民共和国民法典》、《中华人民共和国政府采购法》和《中华人民共和国政府采购法实施条例》，遵循平等、公平、诚信的原则，甲乙双方协商一致，签订本合同，并共同遵守履行本合同约定条款。

第一条 合同内容

网络安全设备，明细详见合同附件。

第二条 合同金额及付款方式

1、合同价：肆拾叁万贰仟叁佰元整（￥432300.00元）。

2、合同价包括设备费、运费、保险费、搬运费、安装调试费、人员培训费、利润、税金等一切直接和间接的费用。

3、付款方式：项目验收合格后，甲方一次性支付全部货款。乙方向甲方提供全额发票及供货清单，甲方收到后通过银行转账方式予以结算。

第三条 交货期限及地点

1、合同签订后30个日历日内全部到货并安装，随时进行验收，验收完毕出具验收证明。

2、乙方不能按时交货的，甲方有权延期付款并按合同总额收取每天0.01%的违约金。

3、交货地点：甲方指定地点。

第四条 知识产权

乙方保证在本项目中使用的任何技术、产品和服务（包括部分使用），不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由乙方承担所有相关责任。

第五条 包装及运输

1、乙方负责货物到达指定交货地点前的所有包装、运输、装卸及保险事项，相关费用包括在合同总价中。

2、乙方提供货物运送至甲方指定地点所需要的包装，以防止货物在运转中损坏。这类包装应采取防漏、防晒、防腐蚀、防震动及防止其它损坏的必要保护措施。乙方应承担由于其包装或其防护措施不妥而引起货物锈蚀、损坏和丢失的损失责任和费用。

3、货物的运输方式由乙方自行选择，包装须满足货物运输和装卸的要求，保证甲方收到的是无任何损伤的货物，否则因此造成的损失由乙方自行承担。

第六条 质量保证及售后服务

1、质量保证期：终验合格后 36 个月（参数中有具体要求的，按参数要求提供质保）。

2、乙方确保供应设备符合国家标准，如出现不符合，乙方将承担一切责任。

3、乙方承诺的质保期起始时间为终验合格之日。

4、乙方提供的所有设备及辅材必须是未使用过的，使用最新工艺生产的最新产品，质量优良、渠道正当，配置合理。

5、质保期后如需更换零部件，乙方应以优惠价格提供。

6、售后服务：设备如出现问题，在 2 小时内响应，4 小时内到达现场解决问题。在保修期内，免费上门维护和校验。

7、质量保证期内因为产品质量问题产生的所有费用由乙方承担；质量保证期后，乙方保证终生提供及时、优质、价格优惠的技术服务。

8、乙方保证选用的设备技术指标先进、质量可靠，进货渠道正常，配置合理，设备制造所用材料及辅材均用优质材料并符合我国有关标准。

第七条 施工及验收

1、乙方保证按国家标准进行施工或供货，甲方按此标准进行验收。乙方在交货过程中对用户相关人员进行免费设备使用、操作及维护培训。保证甲方用户充分掌握设备、系统的性能，熟练管理和使用系统，并能进行相应的装备仪器使用、维护和故障排除。

2、设备到货后，乙方须派具备相应资质的工作人员到用户现场进行货物清点、安装调试。

3、设备安装调试完成并验收合格后，甲乙双方签署《设备验收合格报告》。

4、安装、调试、验收等费用计入合同总价款。

5、设备、材料到货后，甲方根据合同要求对设备进行外观验收、确认设备的产地、规格、型号和数量。

6、整个项目安装调试完毕后，乙方进行自检，合格后准备验收文件，并书

面通知甲方。

7、验收合格后，填写政府采购项目设备验收单，并向甲方提交系统实施过程中的所有资料，以便组织验收及甲方日后管理和维护。

8、验收依据：

8.1 招标文件、投标文件、承诺；

8.2 合同；

8.3 国家相应的标准、规范。

第八条 争议的解决

因执行本合同所发生的或与本合同有关的一切争议，双方应通过友好协商解决。如果协商开始后六十（60）天还不能解决，双方可依以下一种方式解决：

1、双方达成仲裁协议，向约定的仲裁委员会申请仲裁。

2、向有管辖权的人民法院起诉。

第九条 违约责任

1、按《中华人民共和国民法典》中的相关条款执行。

2、未按合同要求提供产品或设备质量不能满足技术要求，甲方有权终止合同，并对乙方的违约行为进行追究。

第十条 其他

1、本合同 壹 式 陆 份，甲、乙双方各执 贰 份，咸阳市政府采购中心和咸阳市财政局采购管理科各存档 壹 份；本合同自甲乙双方签字盖章后生效。

2、合同如有未尽事宜，由双方协商解决。

甲方（盖章）：兴平市人民检察院	乙方（盖章）：陕西奥博迪特电子科技有限公司
地　　址：咸阳市兴平市槐里东路	地　　址：西安市碑林区明胜路9号
邮　　编：713100	邮　　编：710054
电　　话：029-38822321	电　　话：029-87825516
传　　真：	传　　真：029-87825516
开户银行：	开户银行：中国银行西安二环世纪星支行
帐　　号：	帐　　号：1036 2642 4146
代表签字：	代表签字：
2026 年 10 月 28 日	年　　月　　日

附件明细清单：

序号	产品名称	品牌型号	技术参数	数量	单价	总 价
一、工作网 2.0 网络安全设备						
1	防火墙	深信服 AF-1000-L2100-6C	（1）产品网络层吞吐量 10G，应用层吞吐量 4G，全威胁吞吐量 1.6G，并发连接数 400 万，HTTP 新建连接数 10 万； （2）产品接口提供 6 个千兆电口 （3）产品提供 3 年原厂软件升级及硬件质保，包含规则库特征库 3 年升级许可。 （4）产品支持 A|A、A|S 两种双机模式部署。双机故障切换时不丢包，双机部署下升级不断网。 （5）为保证核心业务的支持对链路实现负载均衡及健康状态监测功能，可基于 IPSEC VPN 机制完成路由的智能优化与选择。 （6）产品支持从多个层面开展访问控制，涉及的层面包括：网络分区、网络实体、MAC 地址、服务类型、应用程序、域名地址等。 （7）产品具备链路探测功能，可在各接口上通过 PING、DNS、ARP、BFD 等协议对目标主机的可达状态进行探测，以判断链路的有效性； （8）产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。 （9）产品具备僵尸主机检测功能，内置超过 128 万种僵尸网络特征库，能够识别主机的异常外联行为。	1 台	51000.00	51000.00

			（10）产品支持多种方式进行安全日志存储，包括防火墙本机、日志服务器等不同方式进行安全日志存储。 （11）为满足对员工上网行为以及多样化网络应用的精细化管理需求，产品具备对不少于 9213 种应用的识别与控制能力，且支持对 P2P 下载、游戏、购物、图书百科、工作招聘、聊天工具、旅游出行、股票软件等类型应用的检测与控制。 （12）产品支持管理安全策略，可以管理以及审计安全策略修改的时间、原因、变更类型。支持基于用户名/密码和 Key 等不同方式的管理员登陆双因素认证机制。 （13)产品具备 IT 产品信息安全认证证书 EAL4 增强级。 （14）产品的生产厂商参与制定《信息安全技术第二代防火墙安全技术要求》。			
2	边界防火墙	深信服 AF-1000-FH1600B-M4	（1）产品网络层吞吐量 10G，应用层吞吐量 2G，并发连接数 200 万，HTTP 新建连接数 6 万； （2)产品接口提供 8 个千兆电口+2 个千兆光口。 （3)产品提供 3 年原厂软件升级及硬件质保，包含规则库特征库 3 年升级许可。 （4）产品具备链路探测功能，可在各接口上通过 PING、DNS、ARP、BFD 等协议对目标主机的可达状态进行探测，以判断链路的有效性； （5）产品具备对非法、违规网站访问行为的管控能力，并需配备海量的 URL 分类库。 （6)产品具备僵尸主机检测	1 台	31900.00	31900.00

			功能，内置超过 128 万种僵尸网络特征库，能够识别主机的异常外联行为。 （7)产品支持虚拟防火墙的创建、启用、停用、删除等操作；虚拟防火墙可实现独立管理及配置的独立存储；虚拟防火墙具备独立的会话管理、网络地址转换、安全策略等功能。 （8)产品内置专门的漏洞数据库及 17750 种 IPS 漏洞规则集，能够依据漏洞 ID、名称、严重级别、CVE 标识、漏洞说明等信息对漏洞特征详情进行查询，且支持对攻击特征数据库进行自定义配置。 （9）产品支持管理安全策略，可以管理以及审计安全策略修改的时间、原因、变更类型。支持基于用户名/密码和 Key 等不同方式的管理员登陆双因素认证机制。 （10)产品支持 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改。 （11）产品支持从多个层面开展访问控制，涉及的层面包括：网络分区、网络实体、MAC 地址、服务类型、应用程序、域名地址等。 (12)产品内置 4580 种 WEB 应用攻击特征，支持对跨站脚本（XSS）攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。 (13)产品厂商具备中国网络安全审查认证和市场监管大数据中心软件安全开发类一级证书 (14)产品的生产厂商具备云			

			安全成熟度模型 CS-CMMI 5 认证。			
3	入侵防御	深信服 NIPS-1000-L2100-M4	（1）产品网络层吞吐量 10G，应用层吞吐量 4G，全威胁吞吐量 1.6G，并发连接数≥400 万，HTTP 新建连接数 10 万； （2）产品接口提供 6 个千兆电口。 (3)产品提供 3 年原厂软件升级及硬件质保，包含规则库特征库 3 年升级许可。 （4）产品支持对链路实现负载均衡及健康状态监测功能，可基于 IPSEC VPN 机制完成路由的智能优化与选择。 （5）产品支持从多个层面开展访问控制，涉及的层面包括：网络分区、网络实体、MAC 地址、服务类型、应用程序、域名地址等。 （6）产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。 （7）产品具备僵尸主机检测功能，内置超过 128 万种僵尸网络特征库，能够识别主机的异常外联行为。 （8）产品支持多种方式进行安全日志存储，包括防火墙本机、日志服务器等不同方式进行安全日志存储。 （9）产品支持管理安全策略，可以管理以及审计安全策略修改的时间、原因、变更类型。支持基于用户名/密码和 Key 等不同方式的管理员登陆双因素认证机制。 （10）产品的生产厂商软件研发实力通过 CMMIL5 认证。 （11）产品的生产厂商是国	1 台	52600.00	52600.00

			家信息安全漏洞库 CNNVD（一级）技术支撑单位			
4	日志审计	网御星云 Leadsec-RS-HG-1600	一、硬件规格及性能：1U 标准机架式机箱，国产化操作系统及海光 CPU，内存 16GB，6 个千兆电口，4 个千兆光口，2 个扩展插槽（支持选配扩展网卡），1 个 Console 接口，2 个 USB 接口，128Gm SATA+4TB 企业级硬盘，综合日志处理性能 4000EPS，日志采集处理均值 8000EPS。含 50 个授权，提供原厂三年质保服务及设备系统软件升级服务。 二、功能： 1、日志系统支持 SNMP Trap、Syslog、ODBC、JDBC、文件/文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC 等多种采集方式。 2、系统支持 Lotus Domino、Check Point、VMWare 等设备/应用日志采集任务。 3、支持与 Kafka、HDFS、ES、MongoDB 等大数据存储组件对接，实现日志数据传输与采集。 4、支持达梦、人大金仓、南大通用、神州通用等国产化数据库日志采集，同时支持动态表名模式采集。 5、系统内置多种审计分析规则，支持在线/离线地图定位、视网膜图、事件拓扑图等分析工具。 6、支持日志范式化、设备地址与解析文件绑定、全智能范式化解析；支持原始日志自动识别、标准字段映射及解析字段编辑调整。 7、系统支持日志加密压缩传输，采用 SM4 国密加密算法；支持定时转发，支持 FTP、	1 台	80000.00	80000.00

			SFTP、SMB 三种在线远程备份方式。 8、系统支持大屏展示、事件 TOP10 统计、采集趋势图；支持日志存储空间、已存储天数、剩余存储天数等资源监控展示。 9、系统支持报表邮件自动投递、报表调度；内置网络安全法报表、合规报表、告警报表等模板，支持模板自定义。 10、支持资产分类/分组/分域管理，支持手动录入、导入、标签设置；支持根据事件地址自动识别并新增资产入库。 三、资质： 日志审计---网络关键设备和网络安全专用产品安全认证证书； 日志审计--《网络安全专用产品安全检测证书》日志分析类增强级； 厂家 GB/T27922-2011 优秀的售后服务能力证书； 提供三年硬件维保及技术支持服务。			
5	漏洞扫描	深信服 YJ-1000-B1075-M4	(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；接口：提供千兆电口 6 个，千兆光口 2 个，硬盘容量为 128G SSD+4T HDD (2)产品提供 3 年原厂软件升级及硬件质保。 (3)产品支持指定登录用户名和口令进行本地漏扫检查，基线检查和变更检查支持离线检查、跳转机跳转 (4)产品基线检查支持系统类型包括主机类：Windows、Unix、Solaris、HP-Unix、	1 台	66300.00	66300.00

			AIX、 Linux 等；网络设备：华为、H3C、Cisco、Juniper、中兴等；防火墙：华为、天融信、H3C、Fortigate、Cisco、Juniper、迪普防火墙等；数据库：Mysql、DBOracle、Sqlserver、Sybase 等;中间件:Tomcat、IIS、Webservices、Apache、Weblogic、Resin、Nginx 等;虚拟化平台：VMware ESXi、VMware Center、XenServer （5)产品支持扫描识别出运行的服务和端口，内置漏洞库 58000 条以上。支持 CVE、CNVD、CNNVD、BugTraq 等，拥有完备的知识体系 （6)产品支持漏洞扫描、WEB 扫描、弱口令、安全基线检查、变更检查的五合一任务，五者也可任意组合执行任务 （7）产品支持一次性任务、立即任务、周期任务等多种调度方式； （8)产品可自定义扫描时间段，设置禁止扫描时间段后，该时间段内的周期任务、一次执行任务将无法自动执行。可选择多个例外任务。禁扫时间段不会影响例外任务执行。 （9)产品支持对周期任务的多次任务执行结果进行比对，比对结果中详细展示报告间的异同之处 （10）产品的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，风险评估（一级）。			
6	防毒墙	瑞星 RSW-2350	一、防毒墙： 产品类型：硬件，产品为国有品牌，专业反病毒厂商产品，拥有自主知识产权 产品构架：X86 平台，具有	1 台	93500.00	93500.00

			多重病毒过滤技术、虚拟化病毒分析技术等应用基础 多出口：支持多路链路出口 工作环境：温度 0-40 摄氏度、湿度 20-90%非凝结 平均无故障间隔时间： ≥ 50，000 小时 二、硬件参数： 产品规格：1U 标准机箱 硬件平台：双路多核专业网安硬件平台，保障设备处理性能 网络接口： 10/100/1000BASE-T 接口：6 个（支持 2 对 Bypass 接口） 电源：ATX 电源（250W） HTTP 杀毒吞吐：≥300Mbps FTP 杀毒吞吐：≥280Mbps SMTP 杀毒吞吐：≥100Mbps POP3 杀毒吞吐：≥100Mbps 三、系统功能： 产品成熟度：产品采用国内领先的检测过滤技术，并具有专门的安全操作系统 部署模式：支持透明模式和旁路部署模式，透明模式支持多路透明网桥 管理方式：系统管理支持 BS 架构；支持多种管理方式，本地 Console、远程 SSH、HTTPS 等；支持 IPv4、IPv6 两种类型管理地址的配置管理 帐户管理：支持可信地址管理，能够指定管理员管理设备（绑定 IP）；支持登录超时、账号锁定等安全保护；支持三权分立管理模式，权限相对独立不交叉；支持管理员角色权限的自定义，可灵活配置管理员的权限范围；支持本地和 Radius 第三方用户认证；			

			备份与恢复：对系统配置进行备份，恢复备份配置、恢复系统默认值防火墙功能： 防火墙功能：支持防火墙功能，能够实现网络数据的准入准出过滤 安全功能引用：支持通过防火墙安全策略引用不同的安全配置文件，实现指定的安全防护功能 策略模拟：支持安全策略的模拟执行，诊断安全策略的有效性 内容过滤功能： 内容过滤：支持对 TCP、UDP、DNS、HTTP、FTP、SMTP、POP3、SAMBA、IEC104、IEC61850 等协议进行关键字内容过滤 处理策略：可灵活定义过滤数据的处理策略，例：记录日志或阻断 病毒过滤功能： 病毒监测能力：具有针对国内及全球病毒监测网络，具备新病毒及时发现、处置能力及专业技术资源，保障对新病毒的有效拦截及具备先进的病毒分析技术实力 杀毒引擎：具有国内独立自主产权杀毒引擎，专业的网关病毒过滤引擎，保障防毒墙在网关过滤病毒的效率及性能 数据并行处理技术：具有并行数据处理分析技术，可以完成多链路、高流量环境的病毒过滤 病毒库特征码：具有针对国内用户的病毒库，病毒库特征码≥1000 万，检测的病毒数量≥2 亿 支持协议：支持 SMTP、POP3、FTP、HTTP、SAMBA、IEC104、IEC61850 等协议的病毒过			

			滤，支持 IPv6 协议的病毒检测与过滤 多端口过滤技术：可对 SMTP、POP3、FTP、HTTP、SAMBA、IEC104、IEC61850 等协议通过不同端口传输的数据同时具有病毒过滤功能 深度检测技术：支持协议智能检测，对于未预设的端口，可以智能识别其协议，可以在预设端口和协议不匹配时，转为自动识别出的正确协议 自定义特征：支持病毒特征的自定义，通过 MD5 快速检测病毒 区域双向病毒过滤：支持不同区域间双向查毒；例：WAN-LAN 及 LAN-WAN 双向查毒 病毒处理策略：可灵活定义病毒处理策略，例：查毒或阻断 加壳病毒分析：支持虚拟化病毒分析等脱壳技术，对加壳病毒具备识别、检测及阻断能力 未知病毒过滤：拥有对未知病毒识别、检测及阻断能力 病毒过滤策略：支持多层压缩文件中的病毒过滤，可定制压缩层数；可定制不查杀文件类型；支持对病毒文件进行隔离，支持隔离样本的下载病毒过滤白名单：支持定义 IP 地址白名单，对定义的 IP 地址不进行病毒过滤；要求支持定义 URL 白名单，对定义的 URL 不进行病毒过滤；支持邮件白名单，对定义的邮件地址的附件不进行病毒过滤；支持文件 MD5 白名单，对指定 MD5 值的文件不进行病毒过滤；支持病毒			

			名白名单，对指定病毒名的病毒不进行病毒过滤 病毒库升级：支持在线自动、本地手动方式升级以及局域网升级等多种升级模式；在国内有自主的分布式病毒库升级服务器，保障防毒墙系统病毒库升级的可持续性 入侵防御：支持对各种蠕虫病毒攻击的防御。 双归属链路：支持对双归属链路环境的支持，可以满足非对称路由网络环境的需求。 URL 数据同步：双归属链路中的不同链路的两台墙之间支持 URL 数据同步功能。 非代理应用层杀毒技术：保证不改变经过防毒墙数据的任何特征，做到“透明代理”更加透明。 半连接杀毒技术：具备对网络中半连接的数据进行病毒查杀的功能。 抗 DoS 功能： TCP FLOOD 防护：支持 TCP 洪水攻击的防护 UDP FLOOD 防护：支持 UDP 洪水攻击的防护 ICMP FLOOD 防护：支持 ICMP 洪水攻击的防护 处置策略：可灵活定义 DoS 攻击数据的处理策略，例：记录日志或阻断 IoC 检测： IoC 类型：支持 IPv4、IPv6、域名、URL、MD5、SHA256 等多种情报类型的检测 威胁类型：支持 ATP 攻击、Rootkit、下载器、信息窃取、勒索软件、垃圾邮件、广告软件、恶意程序、感染型、木马、未知威胁、流氓软件、漏洞利用、蠕虫、远程控制、			

			间谍软件、释放器、黑客工具等威胁类型的检测 IoC 情报库：支持内置 ATP 情报库、僵木蠕情报库和自定义特征库 白名单：支持 IoC 检测白名单 处理策略：可灵活定义过滤数据的处理策略，例：记录日志或阻断 挖矿检测： 挖矿行为检测：支持依据矿池域名请示进行网络挖矿行为检测；支持依据挖矿 行为特征进行网络挖矿行为检测白名单：支持挖矿检测白名单 处理策略：可灵活定义过滤数据的处理策略，例：记录日志或阻断 安全联动： 访问控制：支持与现使用的终端安全产品的联动，实现终端非安全主机（存在安全风险的主机）的访问控制 数据联动：支持与态势感知、预警系统等数据分析平台联动，实现数据的集中汇总、分析和展示（提供截图） 日志管理： 日志管理：支持病毒事件、IoC 检测、挖矿检测、内容过滤等安全事件上日志的检索查询；支持系统日志、管理日志等审计日志的检索查询） 远程日志：支持 SYSLOG 远程日志服务；支持多 SYSLOG 服务器的配置 四、防毒墙资质： 测试产品认证：具有公安部信息测试认证、中国安全信息产品 EAL1 认证、西海岸产品认证			

二、内网 1.5 网络安全设备						
1	防火墙	网御星云 Power V6000-FWG3000AFT-G010 V3.0	一、规格：1U 机架式设备，双电源，标配 8 个 10/100/1000M Base-TX，8 个千兆光口；内置 64G SSD 硬盘，含 IPSec VPN 和 SSL VPN 模块。 性能：吞吐量：8G，最大并发连接数：500 万，每秒新建连接数：11 万 二、功能： 1、设备支持防护策略统一模板化，预设高、中、低三档防护强度模板，管理员登录 Web 管理界面可一键单击切换不同防护模板。 2、设备搭载专用安全操作系统，支持静态路由；OSPF、RIP、BGP、ISIS 动态路由协议；支持 VLAN 间路由、单臂路由、组播路由。 3、支持一体化复合安全策略，单条策略可同时配置用户认证、流量管控、并发连接限制、新建连接限制、垃圾邮件过滤，减少策略条目，降低运维管理复杂度。 4、多出口场景下，可基于安全区域绑定出接口，针对不同安全区域配置带宽保证策略，保障关键业务带宽。 5、支持 AD 域、POP3、BJCA 单点登录，单点登录服务监听端口可自定义修改。 6、可识别并防护 ICMP、SYN、ACK、SYNACK、UDP 各类泛洪攻击，抵御流量型 DDoS 攻击。 7、支持 MRP 多重冗余协议，具备链路备份、端口冗余、双机热备、集群备份能力，提升网络与设备可靠性。 8、支持 MRP 多重冗余协议，	1 台	57000.00	57000.00

			具备链路备份、端口冗余、双机热备、集群备份能力，提升网络与设备可靠性。 9、支持端口镜像，可将设备任意接口的全部流量镜像转发至本机其他接口，供外接抓包工具进行流量分析。提供截图证明材料。 10、可同时配置多个 Syslog 日志服务器，设备输出日志支持中文。 三、其他： 提供防火墙产品涉密信息系统产品检测证书，并提供检测报告。 提供防火墙产品通过国标 GB/T17626.5 电磁兼容和浪涌冲击抗扰度检测及提供证明材料。 设备含三年硬件原厂保修，为保证后期服务质量，提供厂家 GB/T 27922-2011 优秀的售后服务能力证书			
合计（人民币元）			肆拾叁万贰仟叁佰元整　￥432300.00 元			