采购合同

甲方：延长县人民检察院

乙方：陕西弘达通网络科技有限公司

根据《中华人民国共和国政府采购法》、《中华人民共和国民法典》的相关规定，经甲乙双方协商，就三级等保设备（防火墙、入侵防御、入侵检测、日志审计）达成协议如下：

1、合同概况：

1.1 合同项目名称： 三级等保设备（防火墙、入侵防御、入侵检测、日志审计）。

1.2 合同总价款：小写：366000元；大写：叁拾陆万陆仟元整。

2、供货内容（安装）及交货地点：

2.1 供货内容：详见后附清单

2.2 供货地点：延长县人民检察院指定地点

3、供货期、质保期、质量标准

供货期：合同签订后15天。

质保期：3年。

4、甲方的责任和义务

甲方在采购内容到达指定地点后，甲方应在乙方供货安装完后组织有关人员进行验收，并签署验收单，甲方按合同规定向先乙方支付应付合同价款40%。

5、乙方的责任和义务

5.1 乙方提供货物必须符合国家相关产品质量标准要求，且应达到乙方响应文件中的标准。

5.2 乙方负责在货物验收时保证质量符合甲方要求；

5.3 供货期间产生的所有费用由乙方负责；

5.4 经甲方验收合格后，乙方向甲方移交相关的产品承诺书；

5.5 乙方有权按合同规定向甲方收取应收合同价款；

5.6 该项目所提供的货物，乙方必须保证在质保期内提供免费更换服务。

6、付款方式

本项目预付款为合同总价款的40%。供货完成并验收合格后，7天内支付剩余55%货款，预留5%质保金。

7、合同变更

本合同在双方协商同意的情况下可以变更，具体事宜双方协商确定后签订书面变更、补充协议，本合同和变更、补充协议应当和竞争性谈判文件的实质性内容保持一致。

8、违约责任

8.1 乙方未按期交付货物的，每迟延一日减少合同总价款 1‰，迟延违约金总额不超过合同总价的 10%；迟延超过三十日的，甲方有权解除合同。

8.2 乙方所交货物的品种、质量不符合合同规定标准的，甲方有权拒收。

8.3 质保期内乙方货物出现任何质量问题，乙方不及时解决的，甲方有权拒付质保金。

8.4 甲方未按合同约定付余款，逾期按未付部分应按日向乙方支付0.5‰的违约金。

9、质量保证

9.1 乙方保证按合同规定的品种、数量、参数提供货物；

9.2 本合同规定货物质量标准以及售后服务均按原厂标准执行。质保期内，乙方承担免费更换义务，但因甲方人为因素损坏除外 ；质保期内经确定，因质

量问题给甲方造成的损失，由乙方承担。 质保期后，乙方提供售后服务，费用由甲方支付。

10、不可抗力、意外变故

如果合同双方因不可抗力意外而被阻不能履行其职责，合同期的时间按照不可抗力变故的时间而顺延，或根据实际情况双方友好协商解决。

11、解决合同纠纷方式

如甲乙双方在合同履行过程中发生争议，应协商解决，协商不成，可向延安仲裁委员会申请仲裁。

12、未尽事宜，双方协商，达成补充协议，补充协议与本合同具有同等法律效力。

13、本合同一式肆份，甲方贰份，乙方贰份。

甲方：延长县人民检察院

法定代表人：

或授权代表：

地址：

电话：19909112600

2016年10月27日

乙方：陕西弘达通网络科技有限公司

法定代表人：

或授权代表：

地址： 西安市碑林区雁塔路北段8号李家村万达广场1栋1单元12010室

电话： 18681853032

2016年10月27日

附件：

序号	产品名称	品牌、型号	参数	生产厂家	单位	数量	单价（元）	合计（元）	备注
1	下一代防火墙	深信服AF-2000-L2202-FH	标准2U设备，双电源；标配6千兆电口+2万兆光口SFP+；扩展槽位2个； 内存16G；默认支持IPSec VPN和SSL VPN模块（200个并发用户）；质保期（自硬件产品发货之日起，为期36个月）内免费维修。 吞吐量18Gbps，最大并发：600万，每秒新建连接数：16万 支持通过配置向导快速完成设备的配置，使设备快速上线 支持IPv6安全控制策略设置，能针对IPV6的目的/源地址、源服务端口、服务、扩展头属性等条件进行安全访问规则的设置。 支持静态路由，动态路由，VLAN间路由，单臂路由，组播路由等。 支持链路聚合功能，支持802.3ad和静态轮询、热备等多种模式。 支持一体化安全策略配置，可以通过一条策略实现用户认证、IPS、AV、URL过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能,简化用户管理 支持同一个地址对象中可以包含IP、IP段、IP range、排除地址等多种类型。 支持针对单条策略中的源、目的地址进行新建、并发限制，避免病毒爆发占用过多资源，可以针对单IP(或地址范围)进行新建、并发控制。 支持策略命中数显示，并支持通过安全策略命中数范围查询。 支持针对文件类型进行流量管理，至少支持6类如：电影类、音乐类、图片类、文本类、压缩类、应用程序类等。可以针对不同类型的文件配置不同的流量管理规则。包括针对文件类型单独设置最大带宽、保证带宽、协议流量优先级等支持对SQL注入、XSS、Web恶意扫描行为的防护能力，至少包含对弱口令、版本探测、漏洞扫描三种行为的防护能力。 支持主流ICMPFLOOD\SYNFLOOD\ACKFLOOD\SYNACKFLOOD\UDPFLOOD攻击防护。	深信服股份有限公司	台	1	65232	65232	

2	入侵防御	深信服NIPS-2000-L2202-FY	2U上架设备，1个RJ45Console口，1个管理口，1个HA口，具备BYPASS功能的10/100/1000Base-T接口6个，千兆光口4个(不含光模块)，2个万兆光口，2个扩展插槽，2个USB口，双电源，质保期内(自硬件产品发货之日起，为期三年) 免费维修，带三年的入侵防御特征库升级授权。 吞吐量30Gbps，最大并发500万，每秒新建连接数20万 内置专业的入侵防御特征库，覆盖勒索、挖矿、webshell、僵尸网络、木马后门、蠕虫、信息泄漏、权限绕过、未授权访问、文件上传、文件读取、文件下载、文件包含、SSRF、XXE、CSRF、反序列化、代码执行、命令执行、XSS攻击、SQL注入、DOS等攻击类型， 规则应支持至少包括规则ID、规则名称、威胁级别、动作、威胁类型、发布时间等条件进行筛选 支持黑白名单，至少包括IP、域名、URL等四种类型，应支持黑白名单全局检索，输入条件可直接查询黑白名单记录支持WEB过滤，对web内容，传输文件名称、传输文件内容过滤，应支持邮件过滤，对邮件标题、邮件正文、附件名称、附件内容过滤，阻断并支持邮件提醒 支持策略调优，分析日志自动关联配置可一键修订规则动作和模板响应方式，具备详细的策略调优记录包含操作时间、操作模块、操作对象、动作、调优结果等 支持威胁分析功能，通过与威胁情报、全流取证、网络负载、内置解码工具、事件处理流程、事件性质判定等信息综合对威胁进行分析判断。 支持SQL注入防护和XSS攻击防护，检测点至少支持URL、Cookie、Reference、Form、User-Agent、X-Forwarded-For，内置AI检测模型，利用机器学习技术对SQL注入报文进行分析，检测和识别SQL注入行为。 支持HTTP协议自适应解码、URL解码、base64解码、XML解码、Unicode解码、十六进制转换、CHR解码、UTF-7解码，支持解析7层以上混合编解码能力，可实现对多层编码攻击的检测，支持格式文本解析JSON解析、html解析、multipart解析。	深信服股份有限公司	台	1	76168	76168	

			设备监控指标至少包含CPU利用率,内存利用率,硬盘利用率,CPU温度,主机温度,系统连接数,授权有效性,HA主备切换,磁盘利用率,电源温度,日志存储量,风扇转速,接口等。设备监控告警条件应支持持续时间、阈值配置、告警频率，告警方式支持邮件告警和推送到本地消息中心。设备巡检包括硬件巡检、运行状态巡检、安全配置巡检、升级版本巡检、网络巡检、日志巡检等，巡检报告支持邮件与飞书群通知						
3	入侵检测	深信服NIPS-2000-L2202-JC	2U上架设备，1个RJ-45Console口，10/100/1000Base-T接口6个，千兆光接口4个（不含光模块），2个万兆光口，2个USB口，扩展插槽2个，512G SSD硬盘，内存：16G， 冗余电源，质保期内（自硬件产品发货之日起，为期36个月）免费维修，含三年的特征库升级授权。 最大吞吐量：18Gbps，最大并发：400万 具备IPv4/IPv6双栈解析能力 支持导入HTTPS、POP3S、IMAPS、SMTPS、RDPS证书,对加密流量进行解密及还原,支持SSL3.0、TLS1.0/1.1/1.2 支持深度协议解析包括http、http2、dhcp、dns、ftp、mysql、imap、bgp、sip、pptp、l2tp等多种通用协议解析，还支持gtpu、ngap、pfcp等5G协议，工控协议的解析，累计支持的深度解析协议种类大于100种 支持对常见的拒绝服务攻击（DOS）的检测能力，针对TCP FLOOD、UDP FLOOD、ICMP FLOOD、DNS FLOOD攻击行为进行检测，并支持通过控制界面配置攻击的检测时间和阈值条件 支持对检测的告警事件结合双向检测机制、原始数据包和关联分析研判模型进行深层次研判给出告警攻击的结果同时根据攻击事件分类给出失陷主机标识,告警结果呈现结果包含五个维度:告警数据展示、基础数据展示、事件描述、云查情报、流量还原； 支持自定义规则，自定义模式支持基础模式和专家模式；可结合用户业务进行深度检测，自定义内容包括源IP、源端口、目的IP、目的端口、协议、事件威胁等级、主机状态、事件类型、检测方向、攻击阶段、攻击结果、攻击手段；支持关联规则分析，进行双向检测规则编写，页面支持下载自定义规则编写说明	深信服股份有限公司	台	1	107417	107417	

			支持全局白名单配置，白名单覆盖范围包括：告警、威胁情报、病毒检测等，可根据流量源目的IP、端口以及协议、协议内容等维度进行灵活的全局过滤策略配置。支持通过页面对告警前后存储报文数量进行配置，并支持启用或禁用情报检测、弱口令检测以及敏感信息检测的pcap包存储功能； 具备数据报表统计能力，报表数据统计方式应从不同的维度进行分析，方便不同层次的技术人员进行数据汇总 具备登录策略功能，允许用户自定义多项登录安全设置，包括设置页面超时自动登出时间、密码的有效期限、密码的最短长度及其复杂度要求、登录时的认证方式、最大允许的登录失败次数以及账户锁定时长，同时还支持配置是否允许多个会话同时使用同一账号登录。						
4	日志分析管理系统	深信服SIP-Logger-L2000	国产化硬件一体机(内置日志审计系统软件和银河麒麟操作系统)。性能：综合日志处理性能：4000EPS，日志采集处理均值：8000EPS。硬件规格：2U标准机箱， 千兆电口6个，千兆光口4个，万兆光口2个，扩展插槽2个，1个Console接口，2个USB接口，双电源，128GmSATA+4TB企业级硬盘。默认包含100个审计对象授权，3年产品基本维保服务。 支持对主流安全设备、网络设备、服务器、终端、数据库、中间件、大数据组件、应用系统等设备系统进行日志采集 支持对日志源进行限速采集，采集过程中支持自定义配置进行采集速率限制，支持带宽限制和速率限制两种模式 支持对范式化字段进行枚举，范式化字段至少包括事件接收时间、用户名称、源地址、源端口、操作、目的地址、目的端口、对象、结果、持续时间、响应、归并条目、事件名称、事件内容摘要、事件分类、等级、原始等级、原始类型、产生时间、网络协议、网络应用协议、设备地址、设备名称、设备类型、程序名称、原始消息、厂商、产品、解析关联等65个字段，字段名称支持自定义； 支持基于规则的关联分析引擎，能够提供逻辑关联、统计关联的关联分析	深信服股份有限公司	台	1	117183	117183	

			能力；关联规则支持规则嵌套和引用，支持多规则联合； 支持查看事件详情，显示日志详情和原始消息；支持以日志详情中的任意字段为筛选条件，快速以该字段为条件对日志进行统计分析； 支持过滤条件和高级搜索模式方式查询，其中过滤条件查询可以对任意日志字段设置禁用、取反等操作；高级查询模式查询需支持单一条件和组合条件复杂查询； 支持拓扑显示配置，拓扑节点标签显示支持名称或IP地址或名称+IP的不同显示模式；支持拓扑维护工具，工具至少包含快速添加、连线、框选模式、移动模式、鹰眼、布局等功能 支持对日志提供在线/离线地图定位,支持源IP与目的IP分布走向的视网膜图展示,支持事件拓扑分析用于描述整个事件的访问关系及过程,支持多维分析； 支持在数据存储时进行阈值设置，包括存储时间不能少于180天、使用容量告警、剩余容量告警、删除方式等设置； 内置报表模板，可预览、导出；系统内置报表编辑器，可以自定义报表，报表类型包括告警统计报表、日志统计报表、日志趋势报表、日志明细报表。						
5	总计：（大写）叁拾陆万陆仟元整						（小写）¥:366000元		

以下为空白！