**许昌市检察院网络建设项目招标要求**

## 一、投标人资格条件

（一）符合《中华人民共和国政府采购法》第22条的规定。

（二）本次招标不接受联合体投标。

（三）根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》 (财库[2016]125 号)的规定，对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，拒绝参与本项目政府采购活动。

## 二、采购需求表

|  |
| --- |
| **一、外网网站系统等级保护建设** |
| 序号 | 设备名称 | 技术指标及规格参数 |
| 1 | 防火墙（1台） | 1.★标准机架式结构型；默认不少于6个10/100/1000BASE-T接口和2个SFP插槽；不少于1个扩展槽位；防火墙吞吐率：不少于6Gbps；并发连接数：不少于300万； 2.支持基于源IP地址、目的IP地址、源端口、目的端口、时间、用户、文件、网址、关键字、邮件地址、脚本、MAC地址等多种方式进行访问控制；3.支持对HTTP、SMTP、POP3、FTP等协议的深度内容过滤，支持URL、关键字过滤；支持对移动代码如Java applet、Active-X、VBScript、Java script的过滤；动态端口支持协议：H.323、SIP、FTP、RTSP、SQL\*NET、MMS、RPC、TFTP、PPTP；4.有完善的地址转换能力，可以支持正向、反向地址/端口转换、双向地址转换等；5.支持静态和动态路由，动态路由RIP；静态路由协议支持基于源地址、目的地址、METRIC值、网络接口的路由；6.支持DHCP SERVER/CLIENT/RELAY功能；支持OPSEC或TOPSEC等类似联动协议，能够与主流入侵检测产品进行联动； |
| 2 | Web防火墙（1台） | 1.★标准机架式结构型；默认不少于6个10/100/1000BASE-T接口；并发连接：不少于150万；吞吐率：不少于1Gbps2.OS命令注入、远程文件包含、目录遍历等WEB通用攻击防护SQL注入、跨站脚本等常见WEB应用攻击；3.爬虫防护，能够审计或阻止谷歌、雅虎、百度等20种以上搜索引擎对网站的爬取行为。4.盗链防护，保护网站中的视频类、音频类及图片类等资源不被盗链。支持Cookie防护及Referer防护两种防盗链算法。5.漏洞扫描器扫描防护，能够审计或阻止IBM AppScan及Acunetix Web Vulnerability Scanner漏洞扫描工具对网站的扫描行为。6.恶意扫描防护，能够通过对WEB的请求行为判断是否为恶意扫描。可设置行为参数阀值，超过阀值后自动将攻击IP加为黑名单进行阻断。阻断时间可手动调节。7.HTTP请求限制，协议规范化。支持对HTTP请求长度、请求方法及请求文件类型等进行限制。支持Cookie安全机制。8.支持防护syn flood、tcp flood、udp flood、icmp flood等网络层拒绝服务攻击9.支持缓存页面方式加快访问速度，减轻服务器访问压力、支持负载均衡功能，把访问分担到多台WEB服务器上10.可分被保护服务、时间段查询，查询结果可生成报表、可记录并分析统计网站的详细信息、可根据访问者的源地址统计分析网站页面访问量、文件请求数及访问流量等业务数据、可根据搜索引擎的类型统计分析网站文件请求数及访问流量等业务数据可、根据访问客户端操作系统或浏览器的类型统计分析网站被访问次数等业务数据11.可根据访问客户端的地域统计分析网站文件请求数等业务数据，地域划分类型支持国家地区、中国省区及中国城市、支持对网站最常被访问的网页情况进行统计分析支、持对访问者进入网站及离开网站时访问网页的情况进行统计分析12.可分被保护服务、时间段查询，查询结果可生成报表、可记录各种WEB攻击、DDoS攻击等日志、可分被保护服务、时间段查询，查询可生成报表 |
| 3 | 入侵检测（1台） | 1.★标准机架式结构型；默认至少配置4个10/100/1000BASE-T接口，整机吞吐量：5G，并发连接： 100万；新建连接：3万/秒；2 要求支持VLAN、MPLS、PPPoE网络，能够在该网络环境中检测出攻击事件。要求支持IPv6、IPv6 over IPv4、IPv6和IPv4混合网络，能够在该网络环境中检测出攻击事件。3.要求能够检测包括溢出攻击类、RPC攻击类、WEBCGI攻击类、拒绝服务类、木马类、蠕虫类、扫描类、网络访问类、HTTP攻击类、系统漏洞类等在内的超过3600种攻击事件。4.支持丢弃报文、记录日志、TCP reset等多种响应动作；支持攻击报文取证功能，检测到攻击事件后将原始报文完整记录下来，作为电子证据。5.支持DHCP flood、DNS Flood、CC攻击检测。支持DDOS 机器人自学习功能，学习时间可设置。6.根据数据内容而非端口智能识别包括P2P（迅雷,FlashGet)、即时通讯、流媒体、股票交易、网络游戏、网络电视等在内的超过150种应用；支持对应用协议的阻断和流量管控；支持URL地址分类库，超过600万种。7.支持WEB站点漏洞扫描功能，内置爬虫、支持关键字自学习和HTML分析。 |
| 4 | 上网行为管理（1台） | 1.★标准机架式结构型，默认包括1个可插拨的扩展槽和4个10/100/1000BASE-T接口，接口支持Bypass；吞吐量:不少于1Gbps；最大并发连接数：不少于100万2.支持ISP自动地址表（电信、移动、网通、铁通等）的策略路由的选路方式； 3.链路聚合是将多个以太网物理端口捆绑成一条逻辑端口（即将多个端口捆绑成一个逻辑的端口以增加带宽，同时增加链路备份）。链路聚合通道要求可以捆绑数不少于10个物理端口。4.必须支持详细的告警功能，包含管理员操作日志、设备状态、流量异常、违规网站、违规帖子、违规文件上传、违规邮件发送以及潜在危害的行为告警；5.支持临时账号自动申请功能，方便外来的临时用户使用。支持自动审核和管理员手动审核的核定方法将临时帐户加入到组织结构中。6.能够根据IP地址/IP地址范围/IP子网/地址簿/用户组的配置来控制网络中单个用户的上行会并发会话数、下行并发会话数；7.可根据时间段来对用户进行黑名单的控制。在生效时间段内才进行黑名单的控制. 在生效时间段外, 不对用户的速率和会话进行限制, 用户产生的流量也不记入黑名单的流量配额内. 8.可通过策略来配置对内网特定用户（IP地址/IP地址范围/IP子网/地址簿/用户组）访问某些外网IP地址（IP地址/IP地址范围/IP子网/地址簿/用户组）进行白名单的控制。符合白名单规则的访问。9.可记录基于个人的行为监控，包括：网页标题记录、发贴记录、网页评论记录、在搜索引擎上的搜索记录、网页文件上传记录、URL访问记录、即时通讯的登录信息/聊天内容/文件传输记录、邮件记录（详细内容、附件）、FTP登录信息/上传记录/下载记录； |
| 5 | 漏洞扫描（1台） | 1. ★标准机架式结构型；配置不少于 4个10/100/1000M自适应网口，单个任务可包含1个B类网段，最大允许并发扫描80个IP地址；默认不少于50个，最大允许并发扫描150个线程；默认不少于80个，最大允许15个扫描任务并发；默认不少于10个，检测漏洞数：大于8000，分布式部署中可以向上级服务器上传扫描结果2. 旁路接入网络，无需改变原有的网络架构。产品的使用无需安装任何类似探针的软件、光盘或USB，基于B/S模式通过浏览器就可以对系统进行远程管理控制；3. 可以限制可扫描的IP地址范围；可以限制用户的登录IP地址；提供无限IP扫描；4. 支持智能端口识别；多重服务检测；知识依赖检测；安全优化扫描；断点恢复扫描；拒绝服务脚本顺序扫描；递进式扫描等功能；5. 应支持手动指定http、ftp、smb、snmp、pop3等常见协议的登录口令；自定义扫描所采用的扫描方式；自定义端口扫描的类型、范围等参数；6. 产品可扫描的漏洞应不少于 20000条，其中中文漏洞库不少于6000条，漏洞库与国际CVE标准兼容；7. 支持nessus插件的直接使用，做到与nessus的同步升级，支持用户自己自定义报表模板；支持html(打印)、html(浏览)、word、pdf等多种格式；支持组态报表，支持用户自己以xml形式自定义报表模板；应支持html(打印)、html(浏览)、word、pdf、txt等多种格式； |
| 6 | 网络审计（1台） | 1.★标准机架式结构型，配置接口不少于4个10/100/1000BASE-T接口；吞吐率：不少于500Mbps2.采用旁路部署方式，支持B/S管理方式，无需在被审计系统上安装任何代理3.支持审计协议包括：HTTP、SMTP、POP3、webmail、FTP、Netbios文件共享、NFS共享、Telnet审计、飞信及IM协议等的审计4.支持170种以上国内常见应用协议行为的自动识别与审计记录，支持URL自动分类，内置URL分类库5.HTTP审计事件包括：访问域，URL引用页 ，URL分类 ，HTTP类别，请求文件，请求参数，访问行为，发布内容，请求结果，网页类别，浏览器，服务器，Cookie，返回长度，代理客户端IP，代理上网，HTTP响应时间6.邮件审计：发件人,收件人, 抄送 , 密送, 邮件主题, 附件7.WEBMAIL审计：WEBMAIL发件人，WEBMAIL收件人，抄送，密送，WEBMAIL主题， 邮件正文，附件，服务提供商可以通过模板方式扩充8.共享审计内容：请求主机名，请求主机域名，请求主机操作系统，请求主机共享协议，应答主机名 ，应答主机域名，应答主机操作系统，应答主机共享协议，操作命令， 登陆用户，原文件名，现文件名，文件名 ，文件类型 9.支持系统管理员IP黑白名单，对于无权访问的IP可以隐藏设备自身IP地址 |
| 7 | 安全管理平台（1台） | 1.★性能：10000条/秒日志综合处理性能，事件分析能力>10000条/秒;支持500+设备状态监控;2.支持B/S模式管理安全管理系统;支持SSL加密模式访问安全信息管理系统;支持多级部署。在系统实现多级部署的情况下，可将下级管理中心的一些敏感事件上传至上级管理中心;可识别、处理多种网络、安全厂家的产品日志，并列表说明;支持系统配置导入导出3.可定义资产信息包括：资产名称、资产IP地址、资产类型、扫描节点、安全等级、业务组、厂商和厂商联系人等信息;资产可以按业务类型进行分类;支持资产的自动发现;支持资产告警信息的自动统计和展示;支持资产的导入和导出；4.支持用户和角色的权限管理;支持非法用户设备访问控制策略;支持非法用户访问控制技术，弱口令攻击和暴露破解控制技术，安全有效时间控制技术；支持密码策略定义;5.为了实时监控当前安全动态，事件摘要支持事件类型统计展示、事件级别统计展示、事件趋势分析展示，实时展示最新top10的安全事件；6.支持事件报表管理和安全对象报表管理;支持按时生成报表，并自动将报表发送到负责人的邮箱中；7.支持报表文件格式包括：HTML格式，WORD格式，EXCEL格式，PDF格式;管理员可以查看系统内置的各种类型的报表。系统内置高达500多种报表模板。8.支持告警事件规则的预制管理；支持冗余日志过滤技术和归并技术；为了提高系统的扩展性和灵活性，支持自定义日志存储位置和存储空间预警和告警；  |
| 8 | 网页防篡改系统（1套） | 网站服务区部署，同时web服务安装防护代理软件, 实现网页防篡改功能 |
| 9 | 防雷保安器（1套） | 二级避雷装置1组、三级避雷装置2组 |
| **二、漏洞扫描入侵检测授权续期3年服务** |
| **三、外网核心交换 1台** |
|  | ★系统架构 | 主控、交换硬件分离架构，交换网板槽位数量≥2个, 管理引擎1+1冗余；支持电源冗余，电源槽位数≥4；业务槽位≥4。 |
|  | ★设备性能 | 交换容量≥16Tbps，包转发率≥3000Mpps。 |
| 1. 0
 | 二层功能 | 支持4K个802.1Q VLAN，Super vlan，支持基于端口、MAC、IP子网、协议的VLAN；支持端口的负载均衡、支持LACP，每个链路聚合组支持8个端口。 |
|  | 三层协议 | 支持静态路由、RIP、OSPF、ISIS、BGP和RIPng、OSPFv3、BGP4+等动态路由协议；支持BFD for VRRP/Static/RIP/OSPF/ISIS等。支持MPLS基本功能MPLS L3 VPN。支持IGMP、IGMP Snooping；支持PIM-S、PIM-DM等三层组播协议。持手工隧道、支持ISATAP、支持6to4隧道。 |
|  | ★维护管理 | 主控卡提供CF接口插槽、带外管理和AUX、独立调试接口。 |
|  | ★虚拟化功能 | 支持≥4台横向虚拟化功能，实现多个物理设备虚拟为一个逻辑设备进行管理的虚拟化功能。支持纵向虚拟化功能，接入交换机作为核心交换机的端口扩展板卡进行配置统一管理,最大支持≥100台设备虚拟成一台设备。（提供技术说明和官网功能介绍截图证明）。 |
|  | 可靠性功能 | 支持不中断业务升级ISSU功能 |
|  | 设备管理 | 支持TELNET、SSH、SNMP、RMON等，支持FTP/TFTP文件传输协议。 |
|  | ★设备配置 | (本次配置需求)主控板卡1+1冗余，交换板卡满配，配置千兆电口≥24，配置千兆光口≥24；配置冗余电源，五块同品牌原厂多模光模块。 |
| **四、楼层交换设备5台** |
| 序号 | 指标项 | 指标要求 |
|  | ★硬件规格 | 48个10/100/1000M电口、4个千兆 SFP光接口（独立非复用）；  |
|  | ★设备性能 | 交换容量≥256G 包转发率≥132Mpps |
|  | ★MAC表容量 | ≥30K。 |
|  | 管理维护 | 1个Console配置口、1个micro USB配置接口、1个Reset键 |
|  | 防雷能力 | ≥7KV  |
|  | 二层功能 | 支持4K个VLAN，支持基于MAC、IP子网的VLAN、支持protocol vlan、支持private valn、支持voice vlan、支持Super vlan，QINQ等；支持端口的负载均衡、支持LACP，每个链路聚合组支持8个端口。支持STP/RSTP/MSTP。多对一的端口镜像，远程端口镜像RSPAN，流镜像。 |
|  | ★三层协议 | 支持DHCP SERVER,支持静态路由、RIPV1/V2动态路由。 |
|  | ACL&QOS功能 | 支持标准、扩展ACL，基于MAC的ACL、基于时间的ACL等；支持IP+MAC+端口的绑定，支持SP、WRR、SP+WRR、DWRR、SDWRR等队列技术。 |
|  | ★虚拟化功能 | 支持纵向虚拟化功能，本机可以作为核心交换机的端口扩展板卡进行配置统一管理,与核心设备配合虚拟成一台设备。（提供技术实现说明和官网功能介绍截图证明） |
|  | 设备管理 | 支持SNMP、TELNET、CONSOLE、SSH管理、WEB等方式管理 |

## 三、相关要求

1、货物技术要求中“防火墙”产品具有国家密码管理局颁发的《防火墙产品密码检测证书》，产品厂家具备TL9000通讯行业质量证书，具备有效的CISP和CISSP培训资质，投标文件中提供加盖生产厂商公章的证书及报告复印件；

2、货物技术要求中“web防火墙”产品具有WEB应用防火墙认证证书，投标文件中提供加盖生产厂商公章的证书复印件；

3、投标人实施人员具有公安部颁发的信息安全等级保护安全建设专业技术人员证书；

4、投标人投标文件中须明确所投产品的厂家、产地、品牌、型号、详细参数，**否则为无效投标。**

5、投标人应就该项目完整投标，**否则为无效投标。**

6、随机资料及附件齐全。

7、设备必须符合国家质量检测标准和本招标文件规定标准的全新正品现货，随货物提供《产品合格证》及其它相关质量证明文件。

8、专利权：投标人应保证用户在使用该货物或其任何一部分时不受第三方提出侵犯其专利权、商标权和工业设计权等的起诉。

9、投标人须明确免费包修期，同时应提出故障响应时间，在免费包修期内，同一质量问题连续两次维修仍无法正常使用，投标人必须予以更换同品牌、同型号的全新产品，超过保修期发生故障，用户可自由选择维修单位，如委托给投标人，投标人不得借故推诿，并且维修费不能超过市场平均价格。

10、投标人须明确维修点地址、负责人、联系人和联系电话，维修点具备什么样的维修能力等详细资料。

11、本项目为交钥匙工程（包括设备、材料、元件等购置、安装调试、验收、与其它施工单位协作所产生的费用等），如有招标文件中没有明确，而本项目必须的各种材料、设备、施工器械均应包括在本项目中，采购人不再另行进行支付有关款项。

12、项目交货期为30天，交货地点为采购人指定地点。

13、投标人应制订切实可行的实施计划，并严格按照交货期进行交货。

14、投标人应提供人员培训方案，并组织实施，内容包括（但不限于）安装调试、使用和运行管理、问题检测与修复等。

15、投标人必须成立合理的组织机构，建立健全保障项目顺利实施的各项管理制度和质量保证体系，安排足够的高素质人才参加本项目的建设。

16、在项目机构中应明确各岗位的职责、任职资格，确保工程顺利实施。根据本项目的业务性质，配备具有同类系统建设经验的项目经理、技术总监等人员承担本项目工作。

17、付款方式**（不响应者为无效投标）**

经验收合格付合同总价款的95%，5%免费质保期满一次付清。

18、采购预算：139.7万元，**超出者为无效投标。**

## 四、评分标准

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目 | 标准 | 说明 |
| 一 | 资质资格 | 18分 | 投标人具有信用AAA等级证书的得1分。 |
| 投标人能提供ISO/IEC20000-1:2005服务管理体系认证及ISO/IEC27001信息安全管理认证体系证书的得4分，有其中一项得2分，没有不得分。须提供以上证书复印件并加盖投标人公章，否则不得分。 |
| 投标人能提供涉及国家秘密的计算机信息系统资质甲级证书（系统集成）资质的得4分，能提供乙级证书的得2分，没有不得分。须提供以上证书复印件并加盖投标人公章，否则不得分。 |
| 投标人能提供信息安全服务资质证书（安全工程类一级）的得2分。投标人具有公安部颁发的信息安全等级保护安全建设服务机构能力评估合格证书得2分，没有不得分。须提供以上证书复印件并加盖投标人公章，否则不得分。 |
| “防火墙”产品具有国家密码管理局颁发的《防火墙产品密码检测证书》的得1分，提供IDC 2012-2016年防火墙产品市场占有率前三名的报告证明的得1分，没有不得分。须提供以上证书材料复印件并加盖产品生产厂商公章，否则不得分。 |
| “web防火墙”产品具有WEB应用防火墙认证证书的得1分，没有不得分。须提供证书复印件并加盖产品生产厂商公章，否则不得分。 |
| “防火墙”、“web防火墙”产品厂家具备TL9000通讯行业质量证书得1分，具有有效的CISP和CISSP培训资质得1分，没有不得分。须提供证书复印件并加盖产品生产厂商公章，否则不得分。 |
| 二 | 业绩 | 10分 | 1、投标人提供2015年以来，政府采购招标中，具有安全系统建设相关项目业绩，中标金额100-300万元（含100万元）以上的单个项目得1分；300万元（含300万元）以上的单个项目得2分。最高得分10分（同时提供中标通知书、与最终用户签订的合同及验收报告复印件，其中合同提供合同首页、盖章页、采购内容页、金额页复印件，并加盖投标人公章，否则不得分。） |
| 三 | 实施及售后服务 | 22分 | 本项目实施人员具有信息安全等级保护安全建设专业技术人员证书的，每份得1分，最多得3分，投标文件中提供证书复印件并加盖投标人公章及人员对应社保缴纳证明否则不得分。 |
| 投标人注册地在本省（包括投标公司或其分公司），提供营业执照证明得2分；针对本项目服务团队不少于5人，安排1人为服务经理，服务经理具有ITSS信息技术服务标准认证、ITIL信息技术基础架构库认证、PMP项目管理专业人士资格认证、服务管理认证证书，每提供一项加1分，最多加4分，投标文件中提供证书复印件并加盖投标人公章及人员对应社保缴纳证明否则不得分。 |
| 为本次采购产品提供原厂三年售后服务，投标文件中提供产品原厂商加盖公章的售后服务文件得2分，不提供不得分。 |
| 有人员技术培训计划的，根据计划的详细程度，评为：一般、良好、优秀，分别得分为1分、2分、3分。 |
| 有工程实施计划的，工期进度安排得当，项目实施保障可靠，根据计划的详细程度，评为：一般、良好、优秀，分别得分为1分、2分、3分。 |
| 四 | 产品符合度 | 15分 | 投标产品的技术参数完全满足招标文件要求的得15分；产品的技术参数每负偏差一项扣2分，带★号项每负偏差一项扣4分。 |
| 五 | 产品价格 | 40分 | 满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：投标报价得分=(评标基准价／投标报价)×40 |